



EAST CAMBRIDGESHIRE  
DISTRICT COUNCIL

**Internal Audit Progress and Performance Update**

**October 2022**

## Introduction

- 1.1 The Internal Audit service for East Cambridgeshire District Council provides 210 days to deliver the 2022/23 Annual Audit Plan.
- 1.2 The Public Sector Internal Audit Standards (the Standards) require the Audit Committee to satisfy itself that it is receiving appropriate assurance about the controls put in place by management to address identified risks to the Council. This report aims to provide the Committee with details on progress made in delivering planned work, the key findings of audit assignments completed since the last Committee meeting and an overview of the performance of the audit team.

## Performance

### 2.1 Delivery of the 2022/23 Audit Plan

At the time of reporting, in September 2022, fieldwork is either complete or underway in relation to 45% of the planned work. Delivery remains on track for the year.

Progress on individual assignments is shown in Table 1.

### 2.2 Are clients satisfied with the quality of the Internal Audit assignments?

To date, one survey response has been received in relation to feedback on completed assignments for the 2022/23 audit plan.

### 2.3 Based upon recent Internal Audit work, are there any emerging issues that impact upon the Internal Audit opinion of the Council's Control Framework?

Since the last Committee meeting, the Internal Audit team has finalised a further audit report. The key findings were as follows:

#### **Safeguarding**

Safeguarding, in its broadest sense, is defined as 'to protect from harm'. East Cambridgeshire District Council (ECDC) has a number of duties to safeguard children and vulnerable adults. The purpose of this audit was to provide assurance that the Council has adequate controls in place to fulfil its responsibilities.

The Care Act 2014 sets out a clear legal framework for how local authorities and other parts of the system should protect adults at risk of abuse or neglect and the Children Act 2004 (section 11) places a statutory duty on key people and bodies, including district councils, to make arrangements to ensure that in discharging their functions they have regard to the need to safeguard and promote the welfare of children.

Defined leadership and accountability for safeguarding arrangements are evident across the Council. The Housing and Community Manager has been appointed as the Lead Safeguarding Officer who has overall responsibility for safeguarding children, young people and vulnerable adults on behalf of the Council and there are nine Designated Safeguarding Officers (DSO) across different service areas. The audit, however,

identified opportunities to further enhance the control framework. The Child and Adults at Risk Safeguarding Policy was found to be out of date and three named DSOs are no longer employed by the Council.

Staff and the public are made aware of their duty to report a safeguarding concern and all staff are suitably advised and trained on the signs and symptoms of abuse and how to report them through mandatory induction training. Biennial safeguarding training is also delivered externally to front line staff and various learning opportunities such as workshops, face to face training and online learning are offered to all staff throughout the year. However, it was difficult during the audit to ascertain who had undertaken the relevant training and therefore the Council would benefit from creating a safeguarding training matrix in order to monitor and evidence that training has taken place.

Audit review of a sample of ten employees and ten taxi licence holders established that right to work and ID checks are being undertaken, however the timeliness of staff DBS checks needs to be improved to ensure that certificates are obtained prior to an employee's start date and a risk assessment is formally documented for those instances where a DBS cannot be obtained.

Based on the work performed during the audit, assurance opinions were given as follows:

<b>Assurance Opinion</b>		
<b>Control Environment</b>	<b>Satisfactory</b>	●
<b>Compliance</b>	<b>Satisfactory</b>	●
<b>Organisational Impact</b>	<b>Moderate</b>	●

During this period, the Internal Audit team has also been working on verification of the Council's use of Disabled Facilities Grant (DFG) monies to enable sign off by the deadline of the end of September 2022.

The National Fraud Initiative (NFI) exercise has also been underway during this period and the datasets are to be uploaded based on data held at 30<sup>th</sup> September 2022. Internal Audit has been facilitating and organising the preparation for this exercise to ensure deadlines are met.

Internal Audit has also provided advice on the recent review of counter fraud policies and advised on the development of the Annual Governance Statement.

#### **2.4 Implementation of audit recommendations by officers**

Where an Internal Audit review identifies any areas of weakness or non-compliance with the control environment, recommendations are made and an action plan agreed with management, with timeframes for implementation.

Since the last Committee meeting, seven agreed actions have been implemented by officers. An overview is provided in Table 2.

At the time of reporting, there are 14 actions which remain overdue for implementation. Of these, there are two actions categorised as 'Medium' priority which have more than three months overdue, further details are provided in Table 3.

## 2.5 Real time risk assurances

Internal Audit are delivering a risk targeted rolling assurance programme to support the Council's risk management processes in 2022/23. Risk management and compliance with the Risk Management Strategy is the responsibility of the Council's management but Internal Audit is seeking to provide assurance over the effectiveness of the risk management process via these assurance reviews.

Internal Audit select risk entries listed within the register on a rolling basis and conduct targeted reviews to confirm that the controls listed on the register are (a) in place and (b) operating as expected. Given that there is a reliance upon these controls to manage the key risks and achieve the residual risk scores, the validity and effectiveness of the controls listed will be verified and reported back to the Audit Committee in regular progress reporting.

The content of the risk entry is also reviewed with the lead officer to seek assurance that the current scoring and details reflect the risk environment at this time. Any potential changes in risk scoring or content are fed back to the Risk Management Group for discussion/amendment.

The second of the rolling risk assurance reviews has been completed and the risk selected was **C4: Failure to achieve compliance with Data Protection legislation (UK General Data Protection Regulations and Data Protection Act 2018)**.

At the time of reporting, the inherent risk scoring for this entry is 15 (3 for likelihood and 5 for impact) and the residual risk is 8 (2 for likelihood and 4 for impact). As such, the listed controls are claimed to reduce the risk of likelihood and impact. Assurance has been sought over those controls.

The findings for each control are detailed in Table 5. The risk scoring was not amended as a result of this review.

A RAG (red, amber, green) rating – as defined below Table 5 – has been assigned to each control. The listed controls were assessed as 'green' with the exception of controls related to staff and Member training and the Record of Processing Activity (ROPA) – where testing highlighted that compliance with the controls was not fully evidenced.

There were six recommended actions arising from the review, as detailed in Table 5.

**Table 1 - Progress against 2022/23 Internal Audit Plan**

Assignment	Planned start	Status	Assurance sought	Assurance Opinion			Comments
				Control Environment	Compliance	Org impact	
<b>Governance &amp; Counter Fraud</b>							
Counter Fraud support / promotion / policies	Q2	As required					Support on review of policies complete. Awareness week planned for November.
National Fraud Initiative	Q3	In progress					
Risk management support and real time assurances	Q1 – Q4	In progress	Ongoing assurances over the controls listed in the Risk Register and supporting embedding of risk management.	Assurances provided on risk entries throughout the year.			See section 2.5 and Table 5
Annual Governance Statement support	Q1	<b>Complete</b>					
Procurement compliance	Q4	Not started					
<b>Key financial systems</b>							
Bank reconciliation	Q3	Not started					
Creditors	Q3	Not started					
Debtors	Q3	Not started					
Payroll	Q3	Not started					

					<i>Assurance Opinion</i>				
<i>Assignment</i>		<i>Planned start</i>	<i>Status</i>		<i>Assurance sought</i>	<i>Control Environment</i>	<i>Compliance</i>	<i>Org impact</i>	<i>Comments</i>
Treasury management		Q3	Not started						
Budgetary control		Q3	Not started						
<b>Key policy compliance</b>									
Staff claims		Q4	Not started						
Safeguarding		Q1	<b>Final report issued</b>		<p>To provide assurance that adequate and effective controls are in place to mitigate the risks identified below in respect of the Council's safeguarding arrangements:</p> <ul style="list-style-type: none"> <li>- Lack of effective leadership and accountability impacts how the Council manages its safeguarding arrangements;</li> <li>- Inappropriate vetting and training of individuals has the potential to expose vulnerable adults and/or children resulting in harm; or</li> <li>- A safeguarding or child protection issue arises due to inadequate safeguarding protocols and procedures.</li> </ul>	<b>Satisfactory</b>	<b>Satisfactory</b>	<b>Moderate</b>	See section 2.3
Enforcement policy compliance		Q2	Fieldwork complete						
<b>Risk based audits</b>									
Asset related audits – follow up		Q4	Not started						
Performance management		Q4	Not started						

<i>Assignment</i>	<i>Planned start</i>	<i>Status</i>	<i>Assurance sought</i>	<i>Assurance Opinion</i>			<i>Comments</i>
				<i>Control Environment</i>	<i>Compliance</i>	<i>Org impact</i>	
Assets of Community Value	Q1	<b>Final report issued</b>	To provide assurance over the Council's consistent and compliant handling of applications for community right to bid.	<b>Good</b>	<b>Substantial</b>	<b>Minor</b>	Reported at July 2022 meeting.
Grant claims	As required	In progress					
<b>IT audits</b>							
IT asset management	Q2	Fieldwork underway					Audit start date delayed due to IT officer availability.
Cyber security	Q4	Not started					

**Table 2 - Implementation of agreed management actions**

	'High' priority recommendations		'Medium' priority recommendations		'Low' priority recommendations		Total	
	Number	% of total	Number	% of total	Number	% of total	Number	% of total
Actions due and <b>implemented</b> since last Committee meeting	2	33%	2	22%	3	50%	7	34%
Actions <b>overdue by less than three months</b>	4	67%	5	55%	2	33%	11	52%
Actions <b>overdue by more than three months</b>	-	-	2	22%	1	17%	3	14%
<b>Totals</b>	<b>6</b>	<b>100%</b>	<b>9</b>	<b>100%</b>	<b>6</b>	<b>100%</b>	<b>21</b>	<b>100%</b>



**Table 3 – Actions overdue more than three months (High or Medium priority)**

Audit plan	Audit title	Agreed action and context	Priority	Responsible officer	Date for implementation	Officer update / revised date
2020/21	Cyber Security	<p><b>Incident management planning</b> There is no specific major malware breach incident plan in place to ensure the most effective and timely response to breaches, limiting impact and enabling recovery to be as effective as possible.</p> <p>Such a plan should include communications with the police and relevant third parties and would inform responses in the case of an incident.</p> <p>An incident management plan should be produced and should include template documentation and logs and details of communications with the police and key partners to support timely action and resolution.</p>	Medium	ICT Manager	31 March 2022	<p>September 22 - Response from ICT Manager:</p> <p>An existing Incident Management Plan formed part of the previous Information Security Policy. This Plan will be reviewed and updated. This has been delayed due to the other pressures within the team working on other projects and issues.</p>
2021/22	ICT Outages	<p><b>Microsoft support package</b> The Council's current package does not provide 24/7 support which means there is an inevitable delay in receiving any support in the case of an outage which commences outside of office hours.</p>	Medium	ICT Manager	31 March 2022	<p>September 22 - Response from ICT Manager:</p> <p>The team have contacted our Microsoft Partners concerning the support current provided and the</p>

Audit plan	Audit title	Agreed action and context	Priority	Responsible officer	Date for implementation	Officer update / revised date
		<p>Given the reliance upon responses from Microsoft, whilst still using an on-premise server, the Council should conduct an options appraisal and cost benefit analysis on packages available against the respective costs.</p>				<p>cost to enhance this support. Microsoft have provided a price for Unified Enterprise Support. However, it is felt that based on the experience of needing Microsoft support in a high level incident, where the team can only recall 3 incidents in the past 18 years, that the increase in cost could not be justified. A report will be presented to Management Team for consideration by the end of October 2022, providing a view on the value for money of the packages available and a recommendation as to how to continue.</p>


### Table 4: Customer Satisfaction

At the completion of each assignment, the Auditor issues a Customer Satisfaction Questionnaire (CSQ) to each client with whom there was a significant engagement during the assignment. There has been one survey response received during the year to date.

Responses	Outstanding	Good	Satisfactory	Poor
Design of assignment	1	-	-	-
Communication during assignment	1	-	-	-
Quality of reporting	1	-	-	-
Quality of recommendations	1	-	-	-
<b>Total</b>	<b>4</b>	<b>-</b>	<b>-</b>	<b>-</b>

**Table 5: Risk register entries – rolling review of controls**

Risk entry			
C4: Failure to achieve compliance with Data Protection legislation (UK General Data Protection Regulations and Data Protection Act 2018).			
Assurance and Findings			
Key control reference	Key control listed on register	RAG rating	Auditor comment and assurances obtained
C4.1	All Council staff and members undertake annual online data protection training. All new staff briefed at Corporate Induction.	● Amber	<p>New starters are provided with a data protection leaflet via ICT at ‘account set up induction’.</p> <p>Annual data protection training is provided by an external training provider (online), with completion records filed.</p> <p>Completion rates were confirmed as: approx. 65% for staff and 7% (2 out of 28) for Members in 2021/22.</p> <p>The Information Governance Officer (Data Protection Officer (DPO)) sends reminders and chases both staff and Member annual training completion.</p> <p>It should be noted that in the case of a data breach, the Information Commissioner would request evidence of training for those involved, as a source of assurance over the organisation’s control framework.</p> <p><b>Recommended actions:</b>  <u>New Starter data protection training</u> - <b>Mandatory</b> online training should be created and completed by all new staff prior to them accessing personal data and within one month of their start date. Completion of this training should be recorded within individual corporate induction records.</p>

Risk entry			
C4: Failure to achieve compliance with Data Protection legislation (UK General Data Protection Regulations and Data Protection Act 2018).			
Assurance and Findings			
Key control reference	Key control listed on register	RAG rating	Auditor comment and assurances obtained
			<p><u>Annual data protection training for all staff</u> – <b>Mandatory</b> annual online refresher training should be completed by all staff with a one month deadline for completion. Completion of this training should be recorded as part of staff training records.</p> <p><u>Annual data protection training for Members</u> – <b>Annual</b> refresher training should be completed by all Members. Completion of this training should be recorded as part of Member training records.</p> <p><u>New Member Induction</u> – <b>Mandatory</b> Data Protection training should be included within the new member induction programme held by the democratic services team. This may be an online training, session with the DPO or a hardcopy exercise. Completion of this training must be recorded as part of Member induction records.</p>
C4.2	Data breach register maintained. All breaches risk assessed, investigated and recommendations made.	 Green	<p>The data breach log has provided assurance that all recorded breaches had been assessed and investigated, with recommendations recorded. The log is sent to the Council's Senior Information Risk Owner (SIRO) monthly for review. However, the DPO has asserted that they would inform the SIRO of any substantial breaches at the time to ensure appropriate reporting to the Information Commissioners Office. Supporting Information provided and reviewed.</p> <p>Guidance and reporting forms are available to all staff via the Council's Intranet.</p>

Risk entry			
C4: Failure to achieve compliance with Data Protection legislation (UK General Data Protection Regulations and Data Protection Act 2018).			
Assurance and Findings			
Key control reference	Key control listed on register	RAG rating	Auditor comment and assurances obtained
C4.3	Record of Processing Activity (ROPA) in place and maintained by Information Officer.	● Amber	<p>A departmental annual ROPA update reminder was sent in January 2022.</p> <p>All departments responded, with the exception of Anglia Revenues Partnership (ARP). The DPO has chased for this information. There is also an expectation that there will have been new information to be added to the ROPA by ARP due to the administration of Covid Grants requiring substantial personal data checks.</p> <p><b>Recommended action</b> that due to the high level of personal data processed by Anglia Revenues Partnership (ARP) in administering local taxation (and considering ARP's involvement in processing test and trace grant payments during the pandemic) it is recommended that this matter is escalated to senior management to resolve so that the Council remains compliant with Article 30 of the GDPR.</p>
C4.4	Data Protection guidance in place and regularly maintained by Information Officer.	● Green	<p>The Council has published information and guidance on both the intranet and internet to cover the relevant areas. Supporting information has been provided and reviewed.</p> <p><b>Recommended action</b> that a review of the information published on the Council's website has identified that further review and updates are required to some published documents – detailed findings shared with officers for actioning.</p>

Risk register entries – rolling review of controls - RAG rating key:

RAG Rating Indicator	
● Red	Control is not present or not currently operating.
● Amber	Control is not operating fully or consistently in line with risk register entry.
● Green	Control in place and evidenced as operating as stated.

## Glossary

At the completion of each assignment the Auditor will report on the level of assurance that can be taken from the work undertaken and the findings of that work. The table below provides an explanation of the various assurance statements that Members might expect to receive.

Compliance Assurances		
Level	Control environment assurance	Compliance assurance
<b>Substantial</b> ●	There are minimal control weaknesses that present very low risk to the control environment.	The control environment has substantially operated as intended although some minor errors have been detected.
<b>Good</b> ●	There are minor control weaknesses that present low risk to the control environment.	The control environment has largely operated as intended although some errors have been detected.
<b>Satisfactory</b> ●	There are some control weaknesses that present a medium risk to the control environment.	The control environment has mainly operated as intended although errors have been detected.
<b>Limited</b> ●	There are significant control weaknesses that present a high risk to the control environment.	The control environment has not operated as intended. Significant errors have been detected.
<b>No</b> ●	There are fundamental control weaknesses that present an unacceptable level of risk to the control environment.	The control environment has fundamentally broken down and is open to significant error or abuse.

Organisational Impact		
Level	Definition	
<b>Major</b> ●	The weaknesses identified during the review have left the Council open to significant risk. If the risk materialises it would have a major impact upon the organisation as a whole.	
<b>Moderate</b> ●	The weaknesses identified during the review have left the Council open to medium risk. If the risk materialises it would have a moderate impact upon the organisation as a whole.	
<b>Minor</b> ●	The weaknesses identified during the review have left the Council open to low risk. This could have a minor impact on the organisation as a whole.	



## **Limitations and Responsibilities**

### ***Limitations inherent to the internal auditor's work***

Internal Audit is undertaking a programme of work agreed by the Council's senior managers and approved by the Audit Committee subject to the limitations outlined below.

### ***Opinion***

Each audit assignment undertaken addresses the control objectives agreed with the relevant, responsible managers.

There might be weaknesses in the system of internal control that Internal Audit are not aware of because they did not form part of the programme of work; were excluded from the scope of individual internal assignments; or were not brought to Internal Audit's attention.

### ***Internal control***

Internal control systems identified during audit assignments, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgement in decision making; human error; control processes being deliberately circumvented by employees and others; management overriding controls; and unforeseeable circumstances.

### ***Future periods***

The assessment of each audit area is relevant to the time that the audit was completed in. In other words, it is a snapshot of the control environment at that time. This evaluation of effectiveness may not be relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in operating environment, law, regulatory requirements or other factors; or
- The degree of compliance with policies and procedures may deteriorate.

### ***Responsibilities of management and internal auditors***

It is management's responsibility to develop and maintain sound systems of risk management; internal control and governance; and for the prevention or detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

Internal Audit endeavours to plan its work so that there is a reasonable expectation that significant control weaknesses will be detected. If weaknesses are detected additional work is undertaken to identify any consequent fraud or irregularities. However, Internal Audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected, and its work should not be relied upon to disclose all fraud or other irregularities that might exist.