



Final Internal Audit Report

East Herts Council - Information Management 2019/20

July 2020

Issued to:	James Ellis – Head of Legal and Democratic Services and Monitoring Officer Dumi Williams – Information and Records Governance Manager Simon Russell – ICT Strategic Partnership Manager Helen Standen – Deputy Chief Executive Bob Palmer – Interim Head of Strategic Finance and Property
Copied to (Final Only):	As above Audit and Governance Committee Members Executive Member for Financial Sustainability
Report Status:	Final
Reference:	E29/19/001
Overall Assurance:	Limited

INDEX

<u>Section</u>	<u>Page</u>
1. Executive Summary	3
2. Assurance by Risk Area	5
Appendix A – Management Action Plan	6
Appendix B – Definitions of Assurance and Recommendation Priorities	11

1. EXECUTIVE SUMMARY

Introduction

- 1.1 Internal Audit provides East Herts Council with an independent and objective opinion on the organisation's governance arrangements, encompassing internal control and risk management, by completing an annual risk-based internal audit plan. This audit formed part of the Council's approved 2019/20 Internal Audit Plan.
- 1.2 The management and use of information have become more important as both the expectations of information governance and the service expected by customers become more demanding. Getting the use and management of information right has a significant part to play in the delivery of the Council's expectations and strategic objectives.
- 1.3 Following the implementation of the General Data Protection Regulation (the GDPR) in May 2018, the Councils could incur financial and reputational damage when information is found to have been poorly managed. The GDPR mandates considerably tougher penalties than the Data Protection Act 1998 (DPA) and organisations can expect fines of up to 4% of annual global turnover or €20 million, whichever is the greater. The UK left the EU on the 31 January 2020 but companies inside the UK will still need to comply with the EU directive until the end of the transition period (end of 2020). Following 2020, UK companies will still need to comply with the principles set out in GDPR as they have been incorporated into the revised Data Protection Act 2018.
- 1.4 The purpose of this audit was to assess the design and effectiveness of the Council's information management controls and the processes for the storage, retention and destruction of paper documents to support compliance with the Council's retention schedule and current legislation.

Overall Audit Opinion

- 1.5 Based on the work performed during this audit, we can provide overall **Limited assurance** that there are effective controls in operation for those elements of the risk management processes covered by this review. These are detailed in the Assurance by Risk Area Table in Section 2 below.

Audit Commentary

- 1.6 Since 2013, the Shared IT Service has been responsible for the provision of IT services to East Herts Council and Stevenage Borough Council. As part of the Council's IT Shared Service Agreement audit in 2019/20, Internal Audit identified an opportunity for both Councils to utilise the shared IT platform to improve services provided to the public by integrating further, specifically in relation to the Shared IT Service and information governance.
- 1.7 Overall responsibility for information management at East Herts Council has been assigned to the Council's Head of Legal and Democratic Services and Monitoring Officer. There is also a Data Protection Officer shared with Stevenage Borough

Council (from November 2019). However, the Council does not have a corporate information governance group or steering committee.

- 1.8 The Council does not appear to have an information asset register in place and has not identified information asset owners for each of its information assets, nor has it defined the responsibilities of the information asset owners. Furthermore, the Council's Information Management Policy is out of date and its Data Breach Policy has not been finalised, approved and communicated to members of staff.
- 1.9 The Council has arrangements in place for ensuring that the principle of least privilege is exercised, and digital information is only accessible and available to those that have a valid business need. It was also observed that there are secure storage facilities for the retention of both electronic and paper documents. However, we found that the Council has not documented the security measures and storage controls for each information asset.
- 1.10 Whilst the Council has a document retention guide in place, it was observed that it is not consistently enforced and applied in practice and we found that the retention schedule is incomplete and out of date. Furthermore, the Council does not have a record of what information has been archived and where it is stored.
- 1.11 The Council has appropriate on-site facilities for confidential waste and for the storage of confidential information. However, it has not defined its procedures for the disposal and destruction of information, including identification and authorisation procedures, nor does it have appropriate confidentiality clauses and contractual agreements with third parties responsible for the disposal and destruction of corporate records.

Summary of Recommendations

- 1.12 We have made one 'High' and three 'Medium' priority recommendations to improve the Council's information management arrangements.
- 1.13 The 'High' priority recommendation relates to the absence of a defined information asset register to capture the Council's information assets and data flows as per the requirements of the GDPR.
- 1.14 The 'Medium' priority recommendations relate to:
 - a) The Council's Information Management Policy is out of date and the Council's Data Breach Policy has not been finalised, approved and communicated to members of staff.
 - b) The Council's document retention schedule is incomplete and out of date and there is no record of the information that has been archived by the Council.
 - c) There are no defined policies or procedures in place for the disposal of information nor are there appropriate confidentiality clauses with third parties.
- 1.15 Please see the Management Action Plan in Appendix A for further details of these recommendations.

Annual Governance Statement

1.16 The findings from this report provide Limited assurance in relation to the Annual Governance Statement and impacts on the Council's ability to ensure compliance with relevant laws and regulations, internal policies and procedures.

2. ASSURANCE BY RISK AREA

2.1 Our specific objectives in undertaking this work, as per the Terms of Reference, were to provide the Councils with assurance on the adequacy and effectiveness of internal controls, processes and records in place to mitigate risks in the following areas:

Risk Area	None	Limited	Satisfactory	Good
Information Governance Whether the Council has a full understanding of what information it holds, why it holds it, what it is used for and its value.				
Storage of Information Whether the Council's information is stored securely and access to information is effectively controlled.				
Retention of Information Whether information and document retention is compliant with the requirements of the General Data Protection Regulation (GDPR).				
Disposal of Information Whether information is securely disposed of and/or destroyed when it is no longer required.				
Overall				

	Finding / Associated Risk	Priority	Recommendation	Management Response	Target Date
1.	<p>Absence of a defined Information Asset Register</p> <p>It was identified during our fieldwork that the Council does not have a defined Information Asset Register in place.</p> <p>We established that the Council has not identified and documented its information assets and data flows, nor has it documented the security measures and storage controls implemented to protect each of its information assets.</p> <p>Furthermore, we established that the Council has not identified appropriate information asset owners, nor has it defined their responsibilities.</p> <p><u>Associated Risk:</u> The absence of a defined information asset register may constitute a breach of the GDPR and exposes the Council to the risk of financial and reputational harm through failure to comply with its regulatory obligations.</p>	High	<p>Management should put arrangements in place for a data audit to be performed, the scope of which should include, but not be limited to, the identification and assessment of the information assets held by the Council.</p> <p>Using the results of the data audit, management should produce an Information Asset Register, which should record the security measures and storage controls implemented to protect each information asset as well as the name of an appropriate information asset owner.</p> <p>Furthermore, management should define the responsibilities of the information asset owners and communicate them to all members of staff.</p>	<p>Responsible Officer: Head of Legal and Democratic Services and Monitoring Officer</p> <p>Management Response: The Head of Legal and Democratic Services and Monitoring Officer had joined the Council days before the audit commenced and it was difficult for him to know precisely where the required information had been saved.</p> <p>While initial searches associated with the audit did not locate an Information Asset Register, one has since been located, as has a list of appropriate information asset owners.</p> <p>The Council is currently reviewing its Information Governance arrangements, following which a review of the Information Asset</p>	September 2020





	Finding / Associated Risk	Priority	Recommendation	Management Response	Target Date
				Register has been prioritised to ensure it is fit for purpose and up to date. This is similarly true for the list of information asset owners as well.	

	Finding / Associated Risk	Priority	Recommendation	Management Response	Target Date
2.	<p>Information Management Policies and Procedures Out of Date</p> <p>It was identified during our fieldwork that the Council's Information Management Policy is out of date. We found that the policy has not been reviewed since it was created in December 2017 and has a scheduled date for review of December 2018.</p> <p>Furthermore, whilst the Council has documented its procedures with regards to data breaches, we found that the Council's Data Breach Policy is in draft and has not been finalised, approved and communicated to members of staff.</p> <p><u>Associated Risk:</u> Where information management policies are incomplete or out of date there is an increased risk that the Council's information will not be managed in line with its strategic objectives and good practice.</p>	Medium	<p>Management should review and where necessary update the Council's Information Management Policy to ensure that it remains relevant to the Council's needs.</p> <p>Furthermore, management should finalise the Council's Data Breach Policy, which should be approved and communicated to all members of staff.</p> <p>The Council should put arrangements in place for reviewing the policies on a routine basis or following a significant change to the Council's operations.</p>	<p>Responsible Officer: Head of Legal and Democratic Services and Monitoring Officer</p> <p>Management Response: Following completion of the aforementioned review of The Council's Information Governance arrangements, it is expected that all policies will be reviewed, updated and finalised shortly.</p> <p>The Head of Legal and Democratic Services and Monitoring Officer is implementing an interactive calendar of policies and procedures which will be viewable on the Council's intranet page to highlight and remind officers when policies are approaching their review date so as to ensure that policies do not become out dated or obsolete.</p>	September 2020

	Finding / Associated Risk	Priority	Recommendation	Management Response	Target Date
3.	<p>Absence of a Defined and Enforced Retention Schedule</p> <p>It was identified during our fieldwork that the Council does not have a defined and enforced retention schedule.</p> <p>Whilst the Council has a document retention guide in place, we established that it is incomplete and out of date and that it is not consistently enforced and applied in practice.</p> <p>Furthermore, it was identified that there is no requirement in place for identifying and recording the information that is being archived by the Council, nor is there a complete record of the information that has been archived to date.</p> <p><u>Associated Risk:</u> The absence of a defined and enforced retention schedule and a record of the information archived by the Council may increase the risk that information will not be managed in line with the requirements of the GDPR.</p>	Medium	<p>Management should review and update the Council's document retention guide so that the corporate retention schedule is in line with the requirements of the GDPR and good practice.</p> <p>Furthermore, management should establish a requirement for identifying and recording any information archived by the Council, including where it is stored, and should put arrangements in place for an archiving log to be developed, maintained and updated on an ongoing basis.</p>	<p>Responsible Officer: Head of Legal and Democratic Services and Monitoring Officer</p> <p>Management Response: Since the completion of the draft audit report, detailed retention schedules and policies have been located for each of the Council's service areas.</p> <p>These are currently being reviewed and will be finalised upon completion of the Council's review of its Information Governance arrangements.</p>	September 2020

	Finding / Associated Risk	Priority	Recommendation	Management Response	Target Date
4.	<p>Absence of Defined Disposal and Destruction Procedures</p> <p>It was identified during our fieldwork that the Council does not have defined policies or procedures in place for the disposal and destruction of information.</p> <p>We established that the Council has not documented its identification and authorisation procedures for the disposal of information, nor has it defined the roles and responsibilities of members of staff and third parties.</p> <p>Furthermore, it was observed that there are no appropriate confidentiality and data protection clauses and contractual arrangements in place with third parties for the disposal and destruction of corporate records.</p> <p><u>Associated Risk:</u> The absence of defined procedures and responsibilities may increase the risk of a data breach occurring as part of the disposal or destruction process, which could result in significant financial and reputational harm.</p>	Medium	<p>Management should define the Council's procedures for the disposal and destruction of information, which should include, but not be limited to, identification and authorisation procedures and the roles and responsibilities of members of staff and third parties.</p> <p>Furthermore, contracts with third parties responsible for the disposal and destruction of corporate records should be reviewed and updated so that they include appropriate confidentiality and data protection clauses.</p>	<p>Responsible Officer: Head of Legal and Democratic Services and Monitoring Officer</p> <p>Management Response:</p> <p>Several contractual documents have also been located since the draft audit report was compiled. These will likewise need to be reviewed in detail, and it is envisaged that this will be undertaken shortly, ideally once the new Information Governance arrangements have been finalised.</p> <p>Until this is finalised, the Head of Legal and Democratic Services and Monitoring Officer is to begin the process.</p>	June 2020

Assurance Level	Definition
Good	The design and operation of the internal control framework is effective, thereby ensuring that the key risks in scope are being well managed and core objectives will likely be achieved. There are minor reportable audit findings.
Satisfactory	The internal control framework is largely working well in managing the key risks in scope, with some audit findings related to the current arrangements.
Limited	The system of internal control is only partially effective, with important audit findings in key areas. Improvement in the design and/or operation of the control environment is necessary to gain assurance risks are being managed to an acceptable level, and core objectives will be achieved.
No	The system of internal control has serious gaps, and controls are not effective in managing the key risks in scope. It is highly unlikely that core objectives will be met without urgent management intervention.

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.