ESSEX FIRE AUTHORITY

Data Retention

FINAL

Internal Audit Report: 9.15/16

4 July 2016

RSM

CONTENTS

Debrief held	23 March 2016	**Internal Audit team**	Daniel Harris - Head of Internal Audit Suzanne Lane - Senior Manager Lee Hannaford - Assistant Manager Hollie Sheppard – Internal Auditor
Draft report issued	21 April 2016		
Responses received	4 July 2016		
Final report issued	4 July 2016	**Client sponsor**	Glenn McGuinness – Deputy Director of Finance
		Distribution	Glenn McGuinness – Deputy Director of Finance

1 EXECUTIVE SUMMARY

1.1 Background

An audit of the Authority's arrangements for Data Retention was undertaken as part of the approved internal audit plan for 2015/16. The objective of the review was to ensure Essex Fire Authority is compliant with data retention requirements and the data protection act principle for data retention.

Principle 5 of the Data Protection Act 1998 requires you to retain personal data no longer than is necessary for the purpose you obtained it for. Ensuring personal data is disposed of when no longer needed will reduce the risk that it will become inaccurate, out of date, or irrelevant.

The Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that:

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

In practice, it means organisations must:

- Review the length of time personal data is kept;
- Consider the purpose or purposes of information held and deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely delete information when it goes out of date.

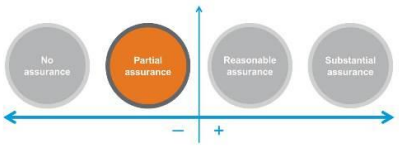
The Authority has an organisation wide Record Retention & Disposal Policy that sets out guidelines for its Members, Officers and employees on how to store records and the retention periods for different categories of records to ensure the principle of the Data protection Act 1998 is met. As part of the review we tested four departments compliance with their current Record Retention & Disposal Policy, these were; HR, Payroll, IT and Finance.

1.2 Conclusion

Testing throughout this audit has highlighted non-compliance with this policy across the four departments and therefore demonstrates a lack of awareness of the Policy and controls in place. Not only did this review find data is retained longer than the approved retention periods but also duplicate data is being held within departments. In addition data retention or protection training is not provided to staff as part of the induction process or locally within departments.

Internal Audit Opinion:

Taking account of the issues identified, the Authority can take partial assurance that the controls to manage this risk are suitably designed and consistently applied.
Action is needed to strengthen the control framework to manage the identified risks.



1.3 Key findings

The key findings from this review are as follows:

- We obtained a screen print from the archive manager system and confirmed the data retention period set on email disposal was three years. We also obtained a screen print from the I.T back-up system that showed back-up files are retained for 12 months after the original data has been deleted. Both system disposal timescales were set in line with the current data retention policy. No records of file disposal are maintained and therefore compliance with this policy cannot be confirmed.

We identified the following areas of weakness which resulted in **one high** and **three medium** priority management actions:

- Discussion and sample testing across the Finance, HR, Payroll and I.T departments found that there is a lack of processes in place to identify when records are due for disposal and data is retained longer than the data retention period set in the policy. In addition, there is a duplication of records being kept. If data is held longer than necessary and there is not sufficient filing and systems in place to identify when data is due for disposal there is a risk that inaccurate data will be retained when it is no longer necessary to hold it, which is a breach of data protection rules. Also holding excessive data is inefficient and Essex Fire Authority must be able to respond to subject access requests for any personal data in line with the data protection act. This may be more difficult if excessive data is held. **(High priority)**.
- The Authority has an organisation wide Record Retention & Disposal Policy that sets out how to store records, the retention periods for different categories of records, and record disposal procedures. On review we noted the Policy does not detail the responsibility of staff for deleting electronic records on key operating systems such as Dream or SAP or the implication of breaching internal timescales and responsibilities set. If the Policy is not regularly reviewed, includes full roles and responsibilities and the implication of breaching internal timescales there is a risk that data will not be retained and disposed in line with current approved requirements **(Medium priority).**
- Essex Fire Authority has not provided any training on data retention or data protection to staff. In the absence of training there is a risk staff will not be equipped to implement the Policy or have sufficient knowledge of the Policy to adhere to it. **(Medium priority)**.
- Records of disposal for electronic or hardcopy data have not been maintained by Payroll and I.T. We were advised that HR and Finance have not disposed of any information to their knowledge. When records of disposal are not maintained there is a risk that the authority cannot monitor departmental compliance with the policy or confirm if records are no longer held where individuals raise information access requests. In addition the organisation may be in breach of the requirements of the Data Protection Act. **(Medium priority)**.

1.4 Additional information to support our conclusion

Risk	Control design*	Compliance with controls*	Agreed actions		
			Low	Medium	High
Data Retention	1 (8)	7 (8)	0	3	1
Total			**0**	**3**	**1**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

2 ACTION PLAN

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may, with a high degree of certainty, lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The table below sets out the actions agreed by management to address the findings:

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
Risk: Data Retention					
1.1	The Record Retention & Disposal Policy is dated December 2013 and has not been reviewed since. The policy states that the review date should have been September 2014. The Policy does not detail: • Who is responsible for deleting electronic records on key operating systems such as Dream or SAP; and • The implication of breaching internal timescales and responsibilities set. Testing throughout this audit has highlighted non-compliance with this policy across all departments and demonstrates a lack of awareness of the Policy.	Medium	The Record Retention & Disposal Policy will be updated to include: • Those responsible for deleting electronic records on key operating systems such as Dream and SAP. and • The implication of breaching internal timescales and responsibilities set. In addition the new policy will be disseminated to all staff and an article published on the staff intranet to emphasise its existence and importance.	Sept 2016	Finance Director & Treasurer

Ref	Findings summary	Priority	Actions for management	Implementation date	Responsible owner
1.3	Essex Fire Authority has not provided any training on data retention or data protection.	Medium	Essex Fire Authority will implement training to all relevant staff on data retention and data protection.	31st March 2017	Learning & Development Manager
1.4, 1.5, 1.6 (a)	There are no processes in place within HR, Payroll and Finance to identify when records are due for disposal. From our testing we have identified that data has been retained longer than the timeframes detailed in the Record Retention & Disposal Policy.	High	Essex Fire Authority will conduct an organisation wide review of data retention. This will include: • Ensuring there are processes in place to identify when records are due for disposal; • Disposing of electronic and hardcopy data in line with the data retention periods in the updated policy; • Making decisions corporately or within departments to hold specific data electronically or in hardcopy so that duplicate records do not exist.	September 2016	Finance Director & Treasurer
1.6. (b)	Contracts Duplicate records have been held electronically and in hardcopy. In addition, data has been retained longer than the data retention period set in policy.		Please refer to management action raised in 1.4 above	31st March 2017	Purchase and Supply Manager
1.8	Records of disposal have not been maintained by Payroll and I.T.	Medium	The Authority will ensure when data is disposed of a record will be kept by departments in line with the Record Retention & Disposal Policy.	31st March 2017	Assistant Director of Finance

3 DETAILED FINDINGS

This report has been prepared by exception. Therefore, we have included in this section, only those risks of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design (yes/no)	Controls complied with (No/N/A)	Audit findings and implications	Priority	Actions for management
Risk: Data Retention						
1.1	Essex Fire Authority (EFA) has an organisation wide Record Retention & Disposal Policy that sets out guidelines for Authority Members, Officers and employees on how to store records and the retention periods for different categories of records. Any decision to retain or dispose of records must be taken in accordance with the guidance within the document. The Policy is dated December 2013 and specifies the date of next review as 30 September 2014 and has not been reviewed. The Policy is available to all staff via the staff intranet.	Yes	No	We obtained the Record Retention & Disposal Policy dated December 2013. Whilst the Policy outlines the current process and some roles and responsibilities of staff are noted it does not detail who has responsibility for deleting electronic records on key operating systems such as Dream or SAP. Also the Policy does not include the implication of breaching internal timescales and responsibilities set. Testing throughout this audit has highlighted non-compliance with this policy across all departments included as part of this review and therefore demonstrates a lack of awareness and understanding of the importance of the Policy. If the Record Retention & Disposal Policy is not regularly reviewed and includes full roles and responsibilities there is a risk that data will not be retained and disposed of in line with current approved requirements and could subsequently lead to the Authority breaching the Data Protection Act which could result in financial penalties. In addition, if the Policy does not include the implication of breaching internal timescales and responsibilities set there is a risk that the importance of data retention will not be understood and implemented correctly by staff.	Medium	Essex Fire Authority will review the Record Retention & Disposal Policy and include: • Those responsible for deleting electronic records on key operating systems such as Dream and SAP. and • The implication of breaching internal timescales and responsibilities set. In addition the new policy will be disseminated to all staff and an article published on the staff intranet to emphasize its existence.

Ref	Control	Adequate control design (yes/no)	Controls complied with (No/N/A)	Audit findings and implications	Priority	Actions for management
1.3	EFA has not provided any training centrally to the organisation on data retention / data protection and the Data Retention Policy. In addition there has been no training provided locally in Finance, HR, Payroll and I.T.	No	N/A	Through discussion with the operational staff and managers in Finance, Payroll, HR and I.T we confirmed the organisation has not provided any training centrally or locally on data retention or data protection. In the absence of training for data retention and protection there is a risk staff will not be equipped to implement the Policy or have sufficient knowledge of the Policy existence to adhere to it..	Medium	Essex Fire Authority will implement training to relevant staff on data retention and data protection.
1.4	The Data Retention Policy requirements in HR are: **EMPLOYEE AND TRAINING RECORDS** All records in relation to employees, including training records, should only be held by the Director of HR and Organisational Development department. Managers should not maintain separate records of employees. • General Retention Period - six years following date employment ceased. The HR system used is SAP and SharePoint is a separate system that is used to hold personal file documentation electronically. HR documentation has been held electronically since SAP was introduced in 2006 so there is no duplication of records.	Yes	No	We obtained a report from SAP that listed all leavers before 1 April 2009 (all records exceeding 6 years). We found this includes all personal details rather than the minimum required. This demonstrated that the electronic record has not been disposed of in line with the Record Retention & Disposal Policy as it is still held on the SAP system. A total of 598 out of date leaver records were retained on SAP. In addition we noted that the hardcopy personnel files for the leavers is archived with the third party storage agency - SALA. We obtained the HR archive spreadsheet information for all hardcopy documents that are currently held by SALA. On review we found 1091 hardcopy leaver personnel files have been retained exceeding the general retention period of six years. If data is held longer than necessary and there is not sufficient filing and flagging systems in place to identify when data is due for disposal there is a risk that inaccurate data will be held and used. In addition when hardcopy data is held longer than required in third party storage there is a risk that the Authority will incur unnecessary storage costs.	High	Essex Fire Authority will conduct an organisation wide review of data retention. This will include: • Ensuring there are processes in place to identify when records are due for disposal; • Disposing of electronic and hardcopy data in line with the data retention periods in the updated policy; • Making decisions corporately or within departments to hold specific data electronically or in hardcopy so that duplicate records do not exist.

Ref	Control	Adequate control design (yes/no)	Controls complied with (No/N/A)	Audit findings and implications	Priority	Actions for management
	One officer inputs the data on SAP and SharePoint and a second officer checks the data is accurate. Hardcopy HR data pre-SAP including personnel files are in storage with the third party storage agency SALA. HR maintains an archive listing individuals personnel files in storage.					
1.5	The Data Retention Policy requirements in Payroll are: **PAYROLL PAY AND ACCOUNTING RECORDS** This category includes all main accounting and payroll records, data entry forms and supporting documentation. • General Retention Period - six years following the close of the financial year. Payroll maintains an archive document that details all documents that are currently held by EDM group a third party storage agency by box reference. The archive spreadsheet details a date of destruction for each box. These destruction dates are not	Yes	No	We confirmed the Payroll archive document could be used for flagging hardcopy data that requires destruction. However, the planned destruction dates are not in line with the data retention policy. The differences in retention periods range from one to four years after the approved period of retention in the Record Retention & Disposal Policy. Hardcopy information held in storage with EDM included: • Overpayment records dated April 2008 - March 2009 which has a destruction date of 1 April 2017; • Debtor invoices dated April 2007 - March 2010 but no destruction date has been given; and • Payment runs / exception reports dated 2008 - 2009 with a destruction date of 1 April 2019. We obtained the hardcopy files in payroll of employee bank detail information and identified that in all five cases the bank details of current and non-current employees had been retained and were dated from 2006 - 31 March 2009.		Please refer to management action raised in 1.01.04.

Ref	Control	Adequate control design (yes/no)	Controls complied with (No/N/A)	Audit findings and implications	Priority	Actions for management
	in line with the data retention policy. Data held manually in storage includes historic debtor invoices, overpayment records and payment runs / exception reports.. Bank detail forms and changes to bank detail requests are kept in hardcopy in a locked filing cabinet in Payroll. These records date from 2006 to date.					
1.6 a	The Data Retention Policy requirements in Finance are: **ACCOUNTING RECORDS** This category includes all main accounting records, including invoices, data entry forms, journals and supporting documentation. • General Retention Period six years following the close of the financial year. The Finance team have been using the financial system Dream since April 2008 which holds key finance documentation such as supplier and debtor records and BACS reports.	Yes	No	We confirmed that the Finance archive document can be used for identifying hardcopy data that requires destruction. However, on review of the spreadsheet we noted that the planned destruction dates are not in line with the data retention policy. Through discussion with the Finance Processes Supervisor and the Financial Processes Manager we confirmed that there has been no disposal of electronic data since Dream was implemented in April 2008. We obtained reports of sales and purchase ledger records from Dream showing data was retained from 1 April 2008 - 31 March 2009 breaching the data retention policy. We obtained the archive spreadsheet of data stored with EDM group. On review we confirmed that hardcopy BACS reports and supplier invoices have been retained from 2008 - 1 April 2009 breaching the data retention policy. We also noted that other key financial documentation is being retained outside the data retention period such as		Please refer to management action raised in 1.01.04.

Ref	Control	Adequate control design (yes/no)	Controls complied with (No/N/A)	Audit findings and implications	Priority	Actions for management
	This has been archived from the old financial system and can still be accessed by the Finance Team. Finance maintain an archive spreadsheet that details all hardcopy data by box reference which is stored offsite with the third party archive agency EDM group. The archive spreadsheet details a date of destruction for each box. These destruction dates are not in line with the data retention policy.			journal and petty cash documents, debtors set up forms and month end reports. We were also advised that weekly BACS files have always been kept in hardcopy but the Finance Team have also scanned the records onto Dream since April 2012 so there is a duplication of data held. We obtained a copy of a weekly BACS file dated 25 February 2016 and confirmed it was held in hardcopy and electronically. We confirmed debtor invoices are also retained in hardcopy and electronically, we were informed that the Authority cannot place reliance on the scanner as it does not accurately copy data. If data is held longer than necessary and there is not sufficient filing and flagging systems in place to identify when data is due for disposal there is a risk that inaccurate data will be held and used. Also holding excessive data is inefficient and EFA must be able to respond to subject access requests for any personal data in line with the data protection act. This may be more difficult if excessive data is held.		
1.6 b	The Data Retention Policy requirements for Contracts are: • General Retention Period - Until three years after the end of the contract. 'Exemptions' Records of insurers will be held on a permanent basis. The Contracts Manager maintains a register of all known contracts that EFA hold.	Yes	No	We obtained the contracts register from the Contracts Manager and noted that there were 131 contracts that had expired more than three years ago dating from January 2006 - 31 March 2014. We reviewed a sample of five of these contracts and confirmed the hardcopy data is still retained on site at EFA headquarters. A further 43 contracts were listed on the contracts register as expired but did not have a date of expiry. Therefore we could not confirm if the data being retained has exceeded the three years retention timescale. Through discussion with the Contracts Manager we were		Please refer to management action raised in 1.01.04.

Ref	Control	Adequate control design (yes/no)	Controls complied with (No/N/A)	Audit findings and implications	Priority	Actions for management
	However, Property Services and IT also maintain their own contracts. Therefore there is no central record of all contracts held by the EFA. The Contracts register details the expiry date of known contracts, so can be used as a flagging system for disposing of contract information in line with the retention timescales. The Contracts Team use the Delta eSourcing procurement portal to advertise contract opportunities and publish awards.			advised that the Contracts Team do not dispose of data so therefore there are no records maintained of disposal. We confirmed that the Contracts team retain contract data electronically and in hardcopy if submitted by the supplier on ePortal. We obtained a copy of a current contract that was held on ePortal and in hardcopy to demonstrate that there is a duplication of records., The Contracts Manager advised that EFA are currently testing a new contracts management database Churwell which has the capacity to store all contract documentation electronically and has the capacity to identify when the data has expired.		
1.7	The Record Retention & Disposal Policy states that: The disposal of all records should be retained detailing the date and method of disposal, and the officer who authorised disposal. For electronic records this should also include the date when the record can no longer be recovered from back-up storage. This record of disposal should be treated as a corporate record.	Yes	No	Through discussion with the Financial Processes Manager and the HR Support Team Manager we were advised the departments have not disposed of data and therefore no records of disposal are held. In addition the I.T Security Officer advised that they were not aware of any disposal of emails and back up data at EFA. The Payroll Manager advised that hardcopy documents have been disposed of in past but this was not recorded. When records of disposal are not maintained there is a risk that the authority cannot monitor departmental compliance with the policy or confirm if records are no longer held to individuals raising information access requests.	Medium	Essex Fire Authority will ensure when data is disposed of a record will be kept by departments in line with the Record Retention & Disposal Policy.

APPENDIX A: SCOPE

Scope of the review

To evaluate the adequacy of risk management and control within the system and the extent to which controls have been applied, with a view to providing an opinion. The scope was planned to provide assurance on the controls and mitigations in place relating to the following risks:

Objective of the risk under review
Compliance with data retention requirements

When planning the audit, the following areas for consideration and limitations were agreed:

Areas for consideration:

The following areas will be considered as part of the review:

- A review of the new policy and compliance testing at a selection of departments/sites to ensure the new policy has been communicated, is understood and is being applied across the service.
- Whether a data retention policy has been developed in line with statutory requirements, and has been reviewed and approved at an appropriate level by the organisation.
- Whether supporting procedures exist that provide adequate guidance to staff at the operational level regarding their responsibilities with respect to data retention.
- Whether the policy and any supporting procedures have been communicated to staff, including training workshops where necessary.
- Whether staff demonstrate awareness of the data retention policy requirements.
- Whether the requirements of the policy are being applied consistently across the organisation this will include the review of 3 areas to include HR and Finance and will determine the following:
    - The record keeping systems currently in use in line with policy,
    - Record retention periods are in line with the policy
    - Determine whether duplicate records exist;
    - Determine whether it is necessary to retain the record; and
    - Identify record creation and disposal concerns.

Limitations to the scope of the audit assignment:

- The audit reviewed the effectiveness of systems in place for the management of data within those areas identified in the areas for consideration above. It does not provide assurance over any other aspects of the records management processes.

- Testing was undertaken on a sample basis.
- We have not confirmed compliance with statutory bodies requirements.
- We have not provided assurance as to whether the requirements within the policy are in line with statutory requirements, only that this as a consideration within the policy.
- Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Elaine Hodgson - Financial Processes Manager
- Kate Roast - Finance Processes Supervisor
- Christopher Massie – ICT Security
- Paul Tye – Contracts Manager
- Angela Mayers - HR Support Team Manager
- Sophie Collins – HR Assistant

FOR FURTHER INFORMATION CONTACT

Name: Suzanne Lane – Senior Manager

Email address: suzanne.lane@rsmuk.com

Telephone number: 07720 508 148

rsmuk.com