



Dacorum Borough Council

Final Internal Audit Report

Data Security

April 2016

This report has been prepared on the basis of the limitations set out on page 12.

CONFIDENTIAL

Distribution List:

John Worts – Information Security Manager
Mark Brookes – Group Manager (Legal Governance)
Steve Baker – Assistant Director (Chief Executive's Directorate) (Monitoring Officer)
David Skinner – Assistant Director (Finance and Resources)
James Deane – Corporate Director (Finance and Operations) (Final Report only)
Sally Marshall – Chief Executive (Final Report only)

Key Dates:

Date of fieldwork: February 2016
Date of draft report: March 2016
Receipt of responses: April 2016
Date of final report: April 2016

This report and the work connected therewith are subject to the Terms and Conditions of the Contract dated 1 April 2015 between Dacorum Borough Council and Mazars Public Sector Internal Audit Limited. This report is confidential and has been prepared for the sole use of Dacorum Borough Council. This report must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law, we accept no responsibility or liability to any third party who purports to use or rely, for any reason whatsoever, on this report, its contents or conclusions.

Contents

1. Executive Summary	1
2. Scope of Assignment	3
3. Assessment of Control Environment.....	4
4. Observations and Recommendations	5
Recommendation 1: Refresher Training (Priority 3)	5
Recommendation 2: Non-Attendance of Training (Priority 3)	6
Recommendation 3: Raising Staff Awareness (Priority 3)	7
Recommendation 4: Printing of Sensitive Data (Priority 2).....	8
Recommendation 5: Unattended Workstations (Priority 2).....	9
Appendix A - Reporting Definitions	10
Appendix B - Staff Interviewed.....	11
Statement of Responsibility.....	12

1. Executive Summary

1.1. Background

As part of the Internal Audit Programme for 2015/16, we have undertaken an audit of the Council's systems of internal control in respect of Data Security.

1.2. Audit Objective and Scope

The overall objective of this audit was to provide assurance over the adequacy and effectiveness of current controls over Data Security, and provide guidance on how to improve the current controls going forward.

In summary, the scope covered the following areas: Policies and Procedures, Training, Storage and Disposal of Personal Data, and Incident Reporting

1.3. Summary Assessment

Our audit of the Council's internal controls operating over Data Security found that there is a sound system of internal control designed to achieve the system objectives. There is also evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk

Our assessment in terms of the design of, and compliance with, the system of internal control covered is set out below:

Evaluation Assessment	Testing Assessment
Full	Substantial

Management should be aware that our internal audit work was performed according to UK Public Sector Internal Audit Standards (PSIAS) which are different from audits performed in accordance with International Standards on Auditing (UK and Ireland) issued by the Auditing Practices Board. Similarly, the assurance gradings provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

Similarly, the assessment gradings provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board. The classifications of our audit assessments and priority ratings definitions for our recommendations are set out in more detail in Appendix A, whilst further analysis of the control environment over Data Security are shown in Section 3.

1.4. **Key Findings**

We have raised four Priority 2 recommendations and one Priority 3 recommendation where we believe there is scope for improvement within the control environment. The recommendations raised have been set out below:

- Staff should receive mandatory refresher training periodically (Priority 2)
- Non-Attendance of Training should be followed up with the relevant Group Manager (Priority 2)
- Council should increase staff awareness relating to information security (Priority 3)
- Officers should collect sensitive documents at the time of printing (Priority 2)
- Officer should not leave workstations logged in when unattended (Priority 2)

Full details of the audit findings and recommendations are shown in Section 4 of the report.

1.5. **Management Response**

We received the management responses in a timely manner and these have been included in the main body of the report.

1.6. **Acknowledgement**

We would like to take this opportunity to thank all staff involved for their time and co-operation during the course of this visit.

2. Scope of Assignment

2.1. Objective

The overall objective of this audit was to provide assurance that the systems of control in respect of Data Security, with regards to the areas set out in section 2.3, are adequate and being consistently applied.

2.2. Approach and Methodology

The following procedures were adopted to identify and assess risks and controls and thus enable us to recommend control improvements:

- Discussions with key members of staff to ascertain the nature of the systems in operation;
- Evaluation of the current systems of internal control through walk-through and other non- statistical sample testing;
- Identification of control weaknesses and potential process improvement opportunities;
- Discussion of our findings with management and further development of our recommendations; and
- Preparation and agreement of a draft report with the process owner.

2.3. Areas Covered

The audit was carried out to evaluate and test controls over the following areas:

Policies and Procedures

The Council has in place a Records Management policy and other associated policies and procedures including a Retention Schedule policy which deals with the secure storage and destruction of personal data. These are regularly reviewed and updated as required.

Training

Frequent, mandatory training of staff is provided and run by the Information Security Manager.

Physical Storage and Disposal of Personal Data

The Council carries out information and physical storage audits to establish the type of personal data being stored and how it is being stored. Arrangements are in place for the secure disposal of confidential waste.









Incident Reporting

Staff are aware of their responsibilities for handling personal data, what constitutes a breach or offence and how to report them using the Council's incident reporting procedure.

3. Assessment of Control Environment

The following table sets out in summary the control objectives we have covered as part of this audit, our assessment of risk based on the adequacy of controls in place, the effectiveness of the controls tested and any resultant recommendations.

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.

Control Objectives Assessed	Design of Controls	Operation of Controls	Recommendations Raised
Policies and Procedures			
Training			Recommendation 1 and 2
Physical Storage and Disposal of Personal Data			Recommendations 3, 4 and 5
Incident Reporting			Recommendations 1 and 3

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.

4. Observations and Recommendations

Recommendation 1: Refresher Training (Priority 2)

<p>Recommendation</p> <p>Management should introduce a requirement for all current staff to complete an Information Security refresher Training session on a regular basis.</p>
<p>Observation</p> <p>In order that members of staff are made aware of their continuing roles and responsibilities regarding Information Security and are kept up to date with any changes in legislative requirements, the Council should require staff to undertake mandatory refresher training on a regular basis, to ensure good working practice.</p> <p>Currently, the Council does not promote refresher training to those employees who have previously received training. Training is currently only promoted as a mandatory requirement for employees to complete within three months of starting with the Council. Consideration should be taken to ensure that all staff who have not received relevant training in the last five years are encouraged to attend the next Information Security training session put on by the Information Security Team Leader.</p> <p>It was confirmed that out of the 15 staff interviewed, from a selection of three service lines within the Council, that 13 had completed the relevant Information Security training. For seven, of the 13 employees, it was confirmed that they had last received training over five years ago. The longest time since receiving Information Security training being in 2004.</p> <p>Where staff do not receive up to date and relevant Information Security training, and are not made aware of where legislative and regulatory requirements have amended, there is a risk of inefficient and out of date working practices being adopted. There is also an added risk of employees not following legislative requirements due to the previous training now being superseded, which may in turn lead to financial penalties being imposed upon the Council.</p>
<p>Responsibility</p> <p>Information Security Team Leader / Training Officer</p>
<p>Management response / deadline</p> <p>The current full training (four sessions per year) is a mandatory requirement for all new staff.</p> <p>We will make the course mandatory every four years for all existing staff to ensure that their training is refreshed.</p> <p>We will review from existing records who has been on the course in the last four years and carry out targeted promotion of the course to ensure attendance. Failure to attend will be followed up with the appropriate Group Manager.</p> <p>Target for reviewing who has/has not been on the course and promotion of the new course will be completed by 1st June 2016.</p>

Recommendation 2: Non-Attendance of Training (Priority 2)

<p>Recommendation</p> <p>Non completion or attendance for mandatory training, should be followed up with the Line Manager of the employee to ensure a legitimate reason for absence is given. Where a response is not received, this should be brought to the attention of the relevant Group Manager.</p>
<p>Observation In order to ensure compliance with the council’s policy regarding mandatory training all staff should inform the trainer / Line Manager of the reason for non-attendance along with confirming attendance at the next available mandatory training session.</p> <p>It was identified from the most recent Information Security training, carried out on the 14th January 2016 that of the 16 people registered to complete the training, only 11 attended, one employee cancelled the morning of training. Four employees did not attend the training session, of which two have given reason for the absence. There was no evidence to confirm that where reasons have not been provided, that this has been followed up and escalated to the appropriate officer.</p> <p>Where staff do not attend mandatory training, there is a risk of ineffective working practices being adopted by employees. This could subsequently have adverse effects on the Council, performance, and in this scenario, data security; an inherent risk for the Council.</p>
<p>Responsibility</p> <p>Information Security Team Leader / Training Officer</p>
<p>Management response / deadline</p> <p>Any non-attendance will be brought to the attention of the employee’s line manager immediately by e-mail from the People team. If an appropriate response is not received this will be reported to the relevant Group Manager. The employee will be automatically booked on the next available course and informed accordingly.</p> <p>The People team currently sends reminder emails to attendees one week before the training course is due. At least 48 Hours’ notice must be given to the People team otherwise the non-attendee’s department will be recharged. This is current practice for external trainers and the recharge procedure for internal training courses will implemented by end of Q1 2016-17.</p>

Recommendation 3: Raising Staff Awareness (Priority 3)

<p>Recommendation</p> <p>The Council should raise staff awareness, potentially through advertisement, of how to determine that documents are classed as confidential or sensitive, distribution of confidential information to other departments, and how to effectively dispose of the confidential or sensitive information.</p>
<p>Observation</p> <p>In order to ensure there are no breaches of Data Security all members of staff should be aware of how to determine what information is classed as confidential, and how to effectively distribute and dispose of sensitive information.</p> <p>It was identified through interviewing five members' staff within three different service lines, 15 staff in total, that on six occasions, staff were unaware of what data is classified as sensitive data. It was further identified that two members of staff did not feel a draft contract was deemed as sensitive, One officer was also unaware of the correct procedure when receiving requests from departments regarding the disclosure of personal information. It was also identified that on two occasions, the officers deemed throwing personal data in a public bin was not a breach of data protection. Audit could not confirm, due to the fact that the forms were anonymous; whether this was because they felt it was an offence under the Data Protection Act and that it did not constitute a breach.</p> <p>Where staff are unaware of the correct procedure for the disposal of confidential waste there is an added risk of a data breach through sensitive information not being disposed securely and confidentially.</p>
<p>Responsibility</p> <p>Information Security Team Leader</p>
<p>Management response / deadline</p> <p>The Information Security Team leader will print the Confidential Information flowcharts and place them above all confidential waste bins. (Action to be completed by 15/4/16).</p> <p>In addition, further communication will be agreed with the Communications team and publicised through the 'Information Station' and 'The Review'. Deadline for both will be 15/4/16.</p> <p>Training is included within the Information Security course on Confidential/Sensitive information and how to treat such information. Making this course mandatory for all staff every four years will help to ensure that staff are fully aware of the relevant procedures.</p>

Recommendation 4: Printing of Sensitive Data (Priority 2)

<p>System Improvement Opportunity</p> <p>The Council should ensure that all members of staff are reminded of the need to ensure that all documents containing sensitive information that they have printed are not be left in the printer area for a prolonged period of time.</p>
<p>Observation</p> <p>In order that security of sensitive data is maintained members of staff should not leave sensitive or confidential information in public areas and to collect documents from the printing areas at the time of printing.</p> <p>During Three Spot Checks of the third floor carried out during 8th February 2016 - 10th February 2016, it was identified that;</p> <p>On two occasions, 9th February 2016 (12:45) and 10th February 2016 (11:30) that sensitive letters were left on the local printer within a department. The letters related to tenant rent arrears and contained sensitive tenant data in each occasion. Audit cannot confirm how long the information was left on the printer for.</p> <p>On one occasion, 10th February 2016 (11:30) that sensitive information in the form of a letter and backing documentation was left on a secure print printer in the corridor of the third floor. Audit cannot confirm how long the information was left on the printer for. It was confirmed that the user must have been present at the printer to release the document, however they failed to collect it at the time of release as no officers were in the corridor at the time of the spot check.</p> <p>Where sensitive data is left in a public area and not stored correctly, there is an increased risk of a breach of the Data Protection Act through leaving sensitive information in potentially public areas where other staff not privy to such information can gain access. This in turn could lead to penalties being imposed where a breach occurs.</p>
<p>Responsibility</p> <p>Information Security Team Leader</p>
<p>Management response / deadline</p> <p>Legal Governance has requested that two communications briefs go out to all staff through the 'Information Station' and 'The Review'. Deadline for both will be 15/04/16.</p> <p>An email will also be sent to all Group Managers to include the same message and ask them to raise the issue in their next team meeting. Deadline 15/04/16.</p> <p>A notice will also be put above all printers to remind staff not to leave any information on printers. Deadline 05/05/16.</p>





Recommendation 5: Unattended Workstations (Priority 2)

<p>System Improvement Opportunity</p> <p>All Computer Users should ensure that they lock their computers when leaving their workstations, this includes short periods of leave from the workstation, such as collecting documents from the printer to ensure good working practice.</p>
<p>Observation</p> <p>In order that the requirements of the Data Protection Act are complied with, members of staff should not leave workstations open and logged in when unattended, this includes short period of leave from the workstation. Staff should ensure they lock their workstations and remove any sensitive information from view when not present at their areas.</p> <p>During three spot checks of the third floor carried out during 8th February 2016 - 10th February 2016, it was identified that on two occasions a Computer User was left logged in to their workstation when not present at their desk. The workstation had live documents open and visible on screen. Audit identified that it was the same desk on the 10th February, 09:00 and 11:30. It cannot confirm how long the user was away from their desk. Also, the desk was viewable from the corridor, where the office door was open.</p> <p>Where workstations are left unattended and logged in, there is an added risk of the security of data being breached. Where employees are working on sensitive materials, and the workstation remains logged in with documents open on the computer screen, there is an increased risk of a data protection breach.</p>
<p>Responsibility</p> <p>Information Security Team Leader</p>
<p>Management response / deadline</p> <p>This area is already covered in the Information Security Training course</p> <p>In addition this matter will also be highlighted in the communications briefs to go out to all staff through the 'Information Station' and 'The Review'. Deadline for both will be 15/04/16.</p> <p>An email will also be sent to all Group Managers to include the same message and ask them to raise the issue in their next team meeting. Deadline 15/04/16.</p> <p>After this the Information Security Team Leader will perform further spot checks and report back to Group Manager – Legal Governance if any issues continue</p>

Appendix A - Reporting Definitions

Audit assessment

In order to provide management with an assessment of the adequacy and effectiveness of their systems of internal control, the following definitions are used:

Level	Symbol	Evaluation Assessment	Testing Assessment
Full		There is a sound system of internal control designed to achieve the system objectives.	The controls are being consistently applied.
Substantial		Whilst there is a basically sound system of internal control design, there are weaknesses in design which may place some of the system objectives at risk.	There is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
Limited		Weaknesses in the system of internal control design are such as to put the system objectives at risk.	The level of non-compliance puts the system objectives at risk.
Nil		Control is generally weak leaving the system open to significant error or abuse.	Significant non-compliance with basic controls leaves the system open to error or abuse.

The assessment gradings provided here are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board and as such the grading of 'Full' does not imply that there are no risks to the stated control objectives.

Grading of recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows:

Level	Definition
Priority 1	Recommendations which are fundamental to the system and upon which the organisation should take immediate action.
Priority 2	Recommendations which, although not fundamental to the system, provide scope for improvements to be made.
Priority 3	Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed.
System Improvement Opportunity	Issues concerning potential opportunities for management to improve the operational efficiency and/or effectiveness of the system.

Appendix B - Staff Interviewed

The following personnel were consulted:

- John Worts Information Security Team Leader
- Matt Rawdon Group Manager (People)
- Andy Vincent Group Manager (Tenants & Leaseholders)
- Chris Baker Group Manager (Revenues, Benefits & Fraud)
- Chris Taylor Group Manager (Strategic Planning & Regeneration)
- Sarah Allen Central Administration Lead Officer
- Ann Stunell Human Resources Team Leader
- Laura Wood Strategic Planning & Regeneration Team Leader
- Stuart Potton Revenues & Benefits Support Team Leader
- Sue Birrell Housing Income Lead Officer
- Jackie Whitefoot Housing Income Officer
- Sharon Scourfield OD & Training Officer
- Nicola Beadle HR Advisor

We would like to thank the staff involved for their co-operation during the audit.

Statement of Responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by us should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Our procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our work and to ensure the authenticity of such material. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

Mazars Public Sector Internal Audit Limited

London

April 2016

This document is confidential and prepared solely for your information. Therefore you should not, without our prior written consent, refer to or use our name or this document for any other purpose, disclose them or refer to them in any prospectus or other document, or make them available or communicate them to any other party. No other party is entitled to rely on our document for any purpose whatsoever and thus we accept no liability to any other party who is shown or gains access to this document.

In this document references to Mazars are references to Mazars Public Sector Internal Audit Limited.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom. Registered in England and Wales No 4585162.

Mazars Public Sector Internal Audit Limited is a subsidiary of Mazars LLP. Mazars LLP is the UK firm of Mazars, an international advisory and accountancy group. Mazars LLP is registered by the Institute of Chartered Accountants in England and Wales to carry out company audit work.