Dacorum Borough Council

Final Internal Audit Report

IT Asset Management

November 2018

This report has been prepared on the basis of the limitations set out on page 9.

CONFIDENTIAL

Distribution List:

Gary Osler – ICT Operations Team Leader

Matt Rawdon – Group Manager, People and Performance

Ben Trueman – Group Manager, Technology & Digital Transformation

Linda Roberts – Assistant Director, Performance, People and Innovation

Nigel Howcutt – Assistant Director, Finance & Resources

James Deane – Corporate Director (Finance and Operations) (Final Report Only)

Sally Marshall – Chief Executive (Final Report only)

Key Dates:

Date of fieldwork:	10th October 2018
Date of draft report:	2nd November 2018
Receipt of responses:	12th November 2018
Date of final report:	13th November 2018

Contents

1. Executive Summary

1.1. Background

As part of the agreed 2018/2019 Audit Plan, Mazars have undertaken a review of the controls in place at Dacorum to ensure that controls have been adequately designed and implemented. IT asset management helps the Council manage their systems more effectively and saves time and money by avoiding unnecessary asset purchases and promoting the efficient use of existing resources.

We are grateful to the ICT Operations Team Leader, and other council staff for their assistance provided to us during the course of the audit.

This report summarises the results of the internal audit work and, therefore does not include all matters that came to our attention during the audit. Such matters have been discussed with relevant staff.

1.2. Audit Objective and Scope

The overall objective of the audit was to evaluate and test controls over the following areas:

- IT Asset Management Policy;
- IT asset register;
- Equipment security;
- Documented procedures; and
- Disposal policy.

Further detail on scope of the audit is provided in Section 2 of the report.

1.3. Summary Assessment

Our audit of DBC's internal controls in operation found that there is a sound system of internal control designed to achieve the system objectives. There is 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.

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 is shown in Section 3.

1.4. Key Findings

Two priority two recommendations were raised where we believe there is scope for improvement within the control environment. These are set out below:

- There should be an annual sample check of the Asset Register and this should be documented for hardware and software (Priority 2).
- A reconciliation should be carried out between Finance and ICT to ensure all assets over the de minimus capital threshold stated within the CMDB (Configuration Management Database) are recorded within the Council's Fixed Asset Register (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. Background

As part of the agreed 2018/2019 Audit Plan, Mazars have undertaken a review of the controls in place at Dacorum Borough Council in relation to IT Asset Management.

2.2. Scope of the Audit

The review focused on providing an independent and objective opinion on the degree to which the Council manages the risks associated with IT asset management, and assessed whether the current arrangements are robust and sufficient relative to the risk identified in relation to the following areas:

- IT Asset Management Policy is in place to aid managing the IT estate, the policy is up to date and available to all IT staff. Responsibility for asset management has been designated.
- All assets are updated to the IT asset register and detailed records are held of hardware equipment and software. The IT asset register is up-to date and an independent annual check of the asset register is completed. Access to the asset register is restricted.
- New equipment or equipment awaiting disposal is held securely, equipment is securely marked and visibly protected. Software licences and original media are held centrally.
- Documented procedures are in place to manage any loss of IT equipment in the council and losses are logged in a database or register.
- A disposal policy and procedure is in place for assets. Disposal facilities are available for the secure disposal of data and IT assets and disposal or destruction certificates are provided.

The audit approach was developed by an assessment of risks and management controls operating within each area of the scope. The following procedures were adopted:

- Identification of the role and objective of each area;
- Identification of risks relating to the auditable area and the controls in place that enable the control objectives to be achieved;
- Evaluation and testing of controls within the system.

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
An IT Asset Management Policy is in place to aid managing the IT estate, the policy is up to date and available to all IT staff. Responsibility for asset management has been designated.			
All assets are updated to the IT asset register and detailed records are held of hardware equipment and software. The IT asset register is up-to date and an independent annual check of the asset register is completed. Access to the asset register is restricted.			**Recommendation 1 (P2)**
New equipment or equipment awaiting disposal is held securely. Equipment is securely marked and visibly protected. Software licences and original media are held centrally.			
Documented procedures are in place to manage loss of IT equipment in the council. Losses are logged in a database or register.			**Recommendation 2 (P2)**
A disposal policy and procedure is in place for assets. Disposal facilities are available for the secure disposal of data and IT assets and disposal or destruction certificates are provided.			

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: Annual sample check of software and hardware assets. (Priority 2).

Recommendation There should be an annual sample check of the Asset register and this should be documented for hardware and software. This could be linked with checks of equipment not logged in for 90 days.
Observation From discussions with the ICT Operations Team Leader, and some compliance testing of the CMDB system, it was found that assets are updated to the IT asset register and detailed records are held of hardware equipment. Software is being recorded on an excel spreadsheet currently. It has been agreed that this will also be transferred over to the CMDB to enable all information to be held in one place. The IT register is kept up-to date by the service desk staff, but there are no annual checks of the asset register being completed to ensure all assets are still held within the council's environment. Where an asset register is not maintained and kept up to date, there is a risk that items will not be appropriately logged for insurance purposes and any losses will not be identifiable.
Responsibility: Group Manager (Technology and Digital Transformation)
Management response / deadline: ICT are happy to accept this recommendation and will undertake and document the first annual sample check at the end of the Financial Year (April 2019). We will link the sample check to check of equipment not logged in for 90 days, using the Dovestones True Last Logon software, which is installed on the Service Desk server.

Recommendation 2: Reconciliation between Finance and ICT assets registers. (Priority 2).

Recommendation

A reconciliation should be carried out between finance and ICT to ensure all assets over the de minimus capital threshold that are stated within the CMDB are recorded within the Council's Fixed Asset Register.

Observation

From discussions with the Accountant and ICT Operations Team Leader, it was noted that IT assets purchased from the ICT capital budget are recorded in the council's fixed asset register and are included within the council's statement of accounts.

Currently there are no reconciliations carried out between finance and ICT to ensure all ICT assets above the de minimus capital threshold are recorded within the Council's fixed asset register, enabling timely depreciation of assets, or maximise ROI.

As finance are not carrying out any reconciliations to the IT asset register, the accountant stated "IT's asset register holds information in greater detail than the fixed asset register. Finance are recording similar groups of equipment as one asset". Reconciling can help to ensure disposals and assets are recorded and valued accurately and correctly.

Responsibility:

Group Manager (Technology and Digital Transformation)

Group Manager (Financial Services)

Management response / deadline:

Finance and ICT will work together to implement a reconciliation process within a 6 month period. The aim of this reconciliation would be to provide assurance that data held in the Council's asset register in respect of IT equipment supports the asset register's purpose - to ensure that assets above our capital de minimus are recorded, valued and depreciated appropriately.

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:

Audit sponsor:	Nigel Howcutt – Assistant Director, Finance & Resources
Audit Contacts:	Matt Rawdon – Group Manager, People and Performance
	Gary Osler – ICT Operations Team Leader
	Andrew Linden – Commissioning, Procurement and Compliance Manager
	Jackie Doyle – Service Accountant

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

Appendix C Statement of Responsibility

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

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.
We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any 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.
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.

This report is confidential and 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 Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or reply for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.