Dacorum Borough Council

Final Internal Audit Report

IT Change Management

July 2019

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

Ben Trueman – Group Manager, Technology & Digital Transformation

Linda Roberts – Assistant Director, Performance, People and Innovation

Nigel Howcutt – 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:	March 2019
Date of draft report:	May 2019
Receipt of responses:	May 2019
Date of final report:	July 2019

Status of our reports

This report ("Report") was prepared by Mazars LLP at the request of Dacorum Borough Council and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of Dacorum Borough Council and 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 rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk. Please refer to the Statement of Responsibility in Appendix C of this report for further information about responsibilities, limitations and confidentiality.

Contents

1. Executive Summary

1.1. Background

As part of the agreed 2018/2019 Audit Plan, Mazars has undertaken a review of the controls in place at Dacorum to ensure controls have been adequately designed and implemented. IT change management helps the Council manage their systems more effectively.

We are grateful to the ICT Operations Team Leader, and other council staff for their assistance provided 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 Change Management Process;
- Software Changes;
- Hardware Changes;

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

- Change Advisory Board meetings/Minutes should be formally recorded/minuted in order for all actions to be monitored by Management (Priority 2).
- An impact analysis should be performed to identify any compatibility issues that may arise through the implementation of new systems or software in the existing ICT infrastructure. Note the timing of this analysis - it should occur before the system/software is procured/developed. (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 has undertaken a review of the controls in place at Dacorum Borough Council in relation to IT Change 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 change management, and assessed whether the current arrangements are robust and sufficient relative to the risk identified in relation to the following areas:

- An IT Change 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 changes to the live environment and the ICT hardware estate should be formally authorised by an appropriate level of management. Consideration should be given to approval from the Finance department for purchases of software or hardware assets. These authorisations/approvals should be formally recorded within the change management documentation. Depending on the classification of the change, it may need to be approved by differing levels of management up to a Change Advisory Board.
- Changes should be scheduled for release into the live environment at times where minimal disruption will be caused to normal working operations. These schedules should cater for both routine and ad hoc changes. Where emergency changes, such as security fixes, are required to be implemented, then these are scheduled at the earliest convenience.
- The compatibility of new/updated systems and software should be assessed against the existing ICT environment prior to the implementation of these changes. Any issues that are identified should be formally documented and taken into consideration as part of the procurement/development process.
- An IT replacement programme promotes the proactive management of the hardware environment through the structured, periodic update of assets to better support the processing requirements of the business. In this manner obsolete equipment is removed from the organisation and the cost of these updates is spread over the lifetime of the replacement programme.

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 Change 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 changes to the live environment and the ICT hardware estate should be formally authorised by an appropriate level of management. Consideration should be given to approval from the Finance department for purchases of software or hardware assets. These authorisations/approvals should be formally recorded within the change management documentation. Depending on the classification of the change, it may need to be approved by differing levels of management up to a Change Advisory Board.	✓	≈	**Recommendation 1 (P2)**
Changes should be scheduled for release into the live environment at times where minimal disruption will be caused to normal working operations. These schedules should cater for both routine and ad hoc changes. Where emergency changes, such as security fixes, are required to be implemented, then these are scheduled at the earliest convenience.	✓	✓	
The compatibility of new/updated systems and software should be assessed against the existing ICT environment prior to the implementation of these changes. Any issues that are identified should be formally documented and taken into consideration as part of the procurement/development process.	✓	≈	**Recommendation 2 (P2)**
An IT replacement programme promotes the proactive management of the hardware environment through the structured, periodic update of assets to better support the processing requirements of the business. In this manner obsolete equipment is removed from the organisation and the cost of these updates is spread over the lifetime of the replacement programme.	✓	✓	

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: Change Advisory Board Minutes formally recorded/minuted. (Priority 2).

Recommendation Change Advisory Board meetings/Minutes should be formally recorded/minuted in order for all actions to be monitored by Management.
Observation From discussions with the ICT Operations Team Leader, it was noted that there are no formally recorded Change Advisory Board minutes, to ensure all actions discussed are captured and all items are actioned accordingly. **Risk:** Change requests may be incorrectly or inconsistently interpreted resulting in uncontrolled or unwarranted changes being implemented. Failure to adequately complete change management records increases the risk that records are not accurate and do not reflect a true picture of the organisation's change state. Therefore, cannot be relied upon.
Responsibility: Group Manager – Technology & Digital Transformation
Management response / deadline The Change process is designed to lead to a binary decision by the Change Advisory Board (CAB) whether to approve or reject a specific change request, rather than free text commentary. Considerable detail (covering the nature and timing of the change, responsibility for its implementation, an assessment of associated risks and planned mitigation) is required by the CAB before a decision on its approval is made. It is unclear how free text minuted records of discussions around these binary decisions would in isolation address the risk that 'Change requests may be incorrectly or inconsistently interpreted…" We firmly commit, however, that where there is any lack of clarity within a change request or where the CAB requires an alteration to the initial request (for example a change in timing or risk mitigation) the initial request will be rejected. A new request, reflecting accurately the expectations of the CAB, will then be required ahead of any approval. In this way, we will ensure that the prescriptive expectations of the CAB are properly recorded within the formal process. **We will ensure this process is followed immediately.**

Recommendation 2: Impact analysis’ not always performed for new system implementations (Priority 2).

Recommendation

An impact analysis should be performed to identify any compatibility issues that may arise through the implementation of new systems or software in the existing ICT infrastructure. Note the timing of this analysis - it should occur before the system/software is procured/developed.

Observation

From discussions with the ICT Operations Team Leader, it was noted that impact analyses are not always carried out for implementation of new systems to identify any compatibility issues which may arise. The ICT Operations Team Leader agreed that all system procurement should come via ICT. Due to cloud based systems now being procured by some managers, this does not always happen.

Risk:

Disruptions or data errors caused by inaccurate specifications or incomplete impact assessment/analysis.

Users not using systems as not meeting their requirements. This results in wasted expenditure as the anticipated benefits are not achieved.

- User requirements are not understood.

Responsibility: Group Manager – Technology & Digital Transformation

Management response / deadline

The ICT SLA (agreed by CMT) lists among ‘Customer Responsibilities’ ‘Ensuring IT related equipment and software is purchased only through ICT’. However, as for historical reasons some technology budgets are held not by ICT but within services’ budgets, the practical application of this responsibility can be challenging.

For this reason, as part of the Council’s New Normal Programme it is planned to establish a Technical Design Authority (TDA). The TDA would sit within the Council’s formal procurement process and would undertake impact assessments at technical, operational and technology strategy levels to the purchase and deployment of any new systems or software.

The establishment of the TDA will form part of a wider review of the Council’s Project Management approach and is expected to be in place in Q3 2019/20.

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:	Linda Roberts – Assistant Director, Performance, People and Innovation
Audit Contacts:	Ben Trueman – Group Manager, Technology & Digital Transformation
	Gary Osler – ICT Operations Team Leader
	Amanda Jefferies – Service Desk/Change Manager

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.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom. Registered in England and Wales No 0C308299.