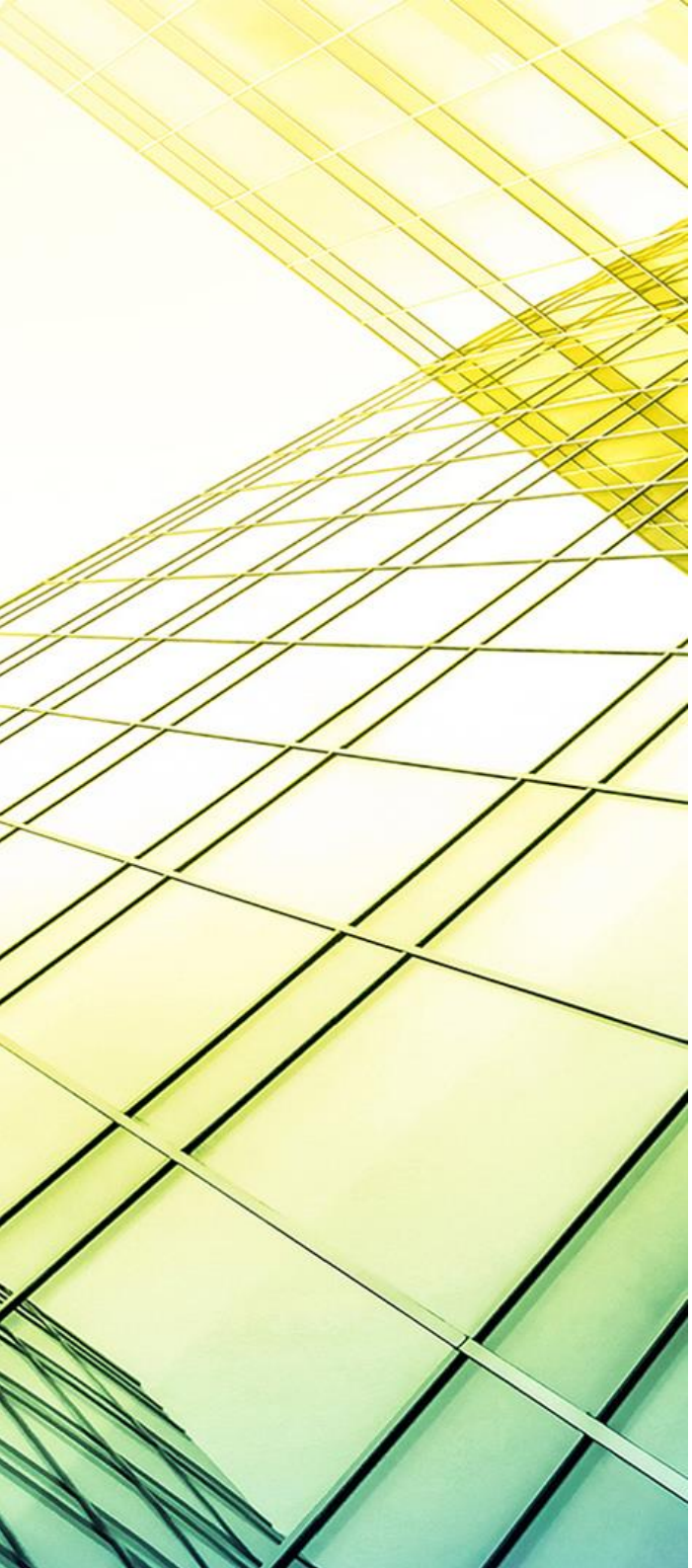
MAZARS

Dacorum Borough Council

Internal Audit Report
IT Disaster Recovery (DR)
March 2020

FINAL REPORT



Contents

Appendices

If you should wish to discuss any aspect of this report, please contact Sarah Knowles, Senior Manager, sarah.knowles@mazars.co.uk or Peter Cudlip, Partner, peter.cudlip@mazars.co.uk

01 Introduction

As part of the agreed 2019/2020 Audit Plan, Mazars has undertaken a review of the IT Disaster Recovery controls in place at Dacorum Borough Council to ensure controls have been adequately designed and implemented. An effective IT DR process supports the objectives of the IT Strategy, which is aligned with business requirements, and helps address underlying IT issues/outages in system and processes.

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.

02 Background

The Civil Contingencies Act 2004 requires that local authorities implement robust Business Continuity arrangements to enable them to continue to provide services and communicate with relevant stakeholders during an incident.

Due to the reliance that is placed on ICT for the operation of services within the Council, ICT service resilience and Disaster Recovery provisions are critical components of Business Continuity.

Disaster Recovery (DR) planning enables the recovery of ICT systems in the event of disruption impacting the data centre or server room hosting the Council's IT systems. Given that information and communication technology plays an increasingly important role in the delivery of Council services, the ability to recover these systems in a timely manner is essential.

Any event that prevents or interrupts an organisation's ability to perform its work tasks is considered a disaster. The moment that ICT becomes unable to support mission-critical processes is the moment the DR plan is invoked to manage the restoration and recovery procedures.

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

- Critical Business Functions and Systems;
- Disaster Recovery (DR) Process;
- Disaster Risk Assessment;
- Disaster Escalation and Emergency Action Procedure;
- Insurance.

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

03 Key Findings

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

Adequacy of System Design	Effectiveness of Operating Controls
	
Substantial Assurance	**Substantial Assurance**

Main Findings

Three priority 2 recommendations and two priority 3 recommendations were raised where there is scope for improvement within the control environment. These are set out below:

- The Disaster Recovery (DR) plan establishes priorities for processing of functions and operations of services. However, the document supplied has not been updated since 2014. (Priority 2).
- The Business Continuity Plan (BCP) does not determine Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) based on business impact. (Priority 2).
- Business Continuity is not included within the induction programme for new key (these would be highlighted by the Resilience Team) employees who may be required to play a part in recovery. (Priority 2).
- Dacorum Borough Council's Disaster Recovery Plan does not contain a section on roles and responsibilities. (Priority 3).
- There are names referenced within the ICT DR plan, however this does not include their contact details. (Priority 3).

Examples of areas of strength

- It was noted that an evaluation and review of the Disaster Risk Assessment to evidence business impact and risk assessments are currently being carried out.
- From discussion with Officers and inspection of documentation there is evidence that Insurance is adequate for Dacorum BC and this also includes business recovery and business impact risks.

Priority	Number of recommendations
1 (Fundamental)	0
2 (Significant)	3
3 (Housekeeping)	2
TOTAL	5

MAZARS

04 Areas for Further Improvement and Action Plan

Definitions for the levels of assurance and recommendations used within our reports are included in Appendix A1.

We identified a number of areas where there is scope for improvement in the control environment. The matters arising have been discussed with the IT Operations Team Leader and the Health, Safety and Resilience Team Leader. The recommendations are detailed in the management action plan below.

	Observation/Risk	Recommendation		Management response	Timescale/ responsibility
4.1	**Identification and agreement of Critical Business Functions.** *Observation*: Inspection of documentation and enquiry of management noted that the Service Level ICT Business Continuity Plan (BCP) does not determine the Recovery Time Objectives (RTO) or Recovery Point Objectives (RPO) of systems based on business impact. It was however noted that the HLDR Schedule does include RTO's and RPOs but that this document had not been updated/reviewed since 2014. All of the required information is contained within the HLDR Schedule; therefore, it may be efficient to use the same information for the IT BCP and to link both documents together. *Risk*: There is a risk that time and point of recovery are not adequately determined or plans do not identify the impact to the business in a disaster scenario for all functions, specifying timescales and priorities for recovering functions, or reflecting the impact any major operational disruption would have on the business.	The ICT Business Continuity Plan should link with an updated version of the ICT High Level Disaster Recovery (HLDR) Schedule in order for Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to be included and identified.	2	The BC plan is due for a review in August 2020. This recommendation will form part of the document review.	August 2020 Group Manager – Technology & Digital Transformation Team Leader Corporate Health, Safety and Resilience

	Observation/Risk	Recommendation		Management response	Timescale/ responsibility
4.2	**IT DR Process.** *Observation*: Inspection of documentation noted that the ICT DR plan establishes priorities for processing of functions and operations of services. However, the document supplied has not been updated with actions since 2014. *Risk*: There is a risk that IT staff/stakeholders may be unaware as to next steps to take if documents are not being reviewed and updated in a timely manner.	All issues raised within the HLDR schedule should be updated and any actions outstanding highlighted to Management as critical. (This recommendation also links to Recommendation 1).	2	The document was updated in 2017 but references to earlier activities had been left in, in error. We will review and update the document as a priority.	April 2020 Group Manager – Technology & Digital Transformation
4.3	**IT DR Process.** *Observation*: Inspection of induction documentation noted that Business Continuity is not included within the induction programme for new key employees who may be required to play a part in recovery if an outage occurs. Training for existing key employees has been adhoc to date but will be rolled out in the future. This should be an annual process. *Risk*: There is a risk that new staff may not be aware of their role or function in a BC scenario.	ICT Management should initiate induction training for new key ICT staff. All key ICT DBC staff likely to be involved in disaster recovery scenarios should complete ICT BC and DR system testing and training annually.	2	ICT have previously committed to IT DR system testing and training and undertake this activity on an annual basis. We will ensure that training on the ICT BCP process is added to this.	June 2020 Group Manager – Technology & Digital Transformation
4.4	**IT DR Process.** Observation: Inspection of documentation noted DBC's ICT DR Plan does not contain a section on roles and responsibilities. The ICT BCP does include a section on responsibility for invocation of the Business Continuity Plan	Job Descriptions should be updated to reflect roles and responsibilities in regard to Business Continuity and Disaster Recovery.	3	ICT will, with support from HR, review job descriptions within ICT to ensure they include appropriate reference to Disaster Recovery.	June 2020 Group Manager – Technology & Digital Transformation

	Observation/Risk	Recommendation		Management response	Timescale/ responsibility
	(including a deputy), as well as responsibility for calling team members (including a deputy). The Health, Safety and Resilience Committee discusses resilience matters and reports to Corporate Management Team. The Corporate Management Team includes the Chief Executive, Directors and Assistant Directors of the Council. The Health, Safety and Resilience Team Leader stated having the Leadership Team involved helps to further enhance and embed those involved in BC in their specific roles within DBC. The Resilience Policy Statement outlines all staff responsible for resilience matters. Enquiry of the IT Operations Manager and inspection of documentation noted there was no evidence of "resource allocation" in the ICT DR Policy/Plan. We did note that the ICT BCP does have "resource allocation" included. From enquiry of management as to whether ICT DR/BC responsibilities had been formally documented within officer's job descriptions, we noted job descriptions have not been updated with ICT DR/BC responsibilities. *Risk*: There is a risk that personnel would be unaware of or fail to act on key responsibilities.				
4.5	**IT DR Process.** Observation: From enquiry and inspection, it was noted that the DCB ICT DR Plan is a high-level plan which mainly details services and agreed critical services with Infrastructure requirements. Although	DBC should consider including a link from the ICT DR Plan to the ICT BCP	**3**	A link to the ICT BCP document has now been added to the IT DR Procedures.	Completed Group Manager – Technology &

	Observation/Risk	Recommendation		Management response	Timescale/ responsibility
	there are names mentioned within the ICT DR plan, there are no further contact details. *Risk:* There is a risk that personnel would not know how to contact key members of staff in the event of a disaster.	document enabling ease of access to all contact information required.			Digital Transformation

A1 Audit Information

Audit Control Schedule	
Client contacts:	Gary Osler – ICT Operations Team Leader Russell Ham - Corporate Health, Safety and Resilience Team Leader Ben Trueman – Group Manager, Technology & Digital Transformation Linda Roberts – Assistant Director, Performance, People and Innovation
Internal Audit Team:	Peter Cudlip, Partner Sarah Knowles, Senior Audit Manager Martin Baird, IT Audit Director Nighat Sheikh, IT Audit Manger
Work commenced	October 2019
Finish on Site \ Exit Meeting:	December 2019
Draft report issued:	February 2020
Management responses received:	February 2020
Final report issued:	March 2020

Scope and Objectives

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

- Critical Priorities - To identify critical business functions and systems identifying and prioritising systems, prioritising critical activities. Ensuring recovery time objectives are being established.

- IT DR Process – There is a review of documentation to be carried out to ensure there is a Business Continuity Strategy, Business Continuity and Disaster Recovery plans and procedures, in place. A consultation is also carried out for the plans. To ensure an approval process is communicated across the organisation. A review to be carried out to ensure there is a competent and qualified designated BC/DR team.

- Business impact and risk assessments - Evaluate and review the Disaster Risk Assessment to evidence business impact and risk assessments are being carried out.

- Disaster invocation/escalation - From discussions with Senior Managers and Team Leaders and inspection of documentation of the Disaster Escalation and Emergency Action Procedure and decision making in regards to the disaster invocation and escalation procedure. To carry out a review of the Incident management plan.

- Insurance cover - Discussion with Officers and inspection of documentation to evidence that Insurance is adequate and includes recovery and business impact risks.

Testing was performed on a sample basis; and as a result, our work does not provide absolute assurance that material error, loss or fraud does not exist.

Definitions of Assurance Levels		
Assurance Level	**Adequacy of system design**	**Effectiveness of operating controls**
Good Assurance:	There is a sound system of internal control designed to achieve the system objectives.	The controls are being consistently applied, or any weaknesses identified do not affect key controls and are unlikely to impair the achievement of the objectives of the system.
Substantial Assurance:	Whilst there is a basic sound system of internal control design, there are weaknesses in design, which may place some of the system objectives at risk.	While controls are generally operating effectively, there are weaknesses, which put some of the system objectives at risk.
Limited Assurance:	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.
No Assurance	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.

Definitions of Recommendations	
Priority	**Description**
Priority 1 (Fundamental)	Recommendations which are fundamental to the system and upon which the organisation should take immediate action. Major issues for the attention of senior management and the Audit Committee
Priority 2 (Significant)	Recommendations, which, although not fundamental to the system, provide scope for improvements to be made. Recommendations for local management action in their areas of responsibility.
Priority 3 (Housekeeping)	Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed. Detailed problems of a minor nature resolved on site through discussions with local management.

A3 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.