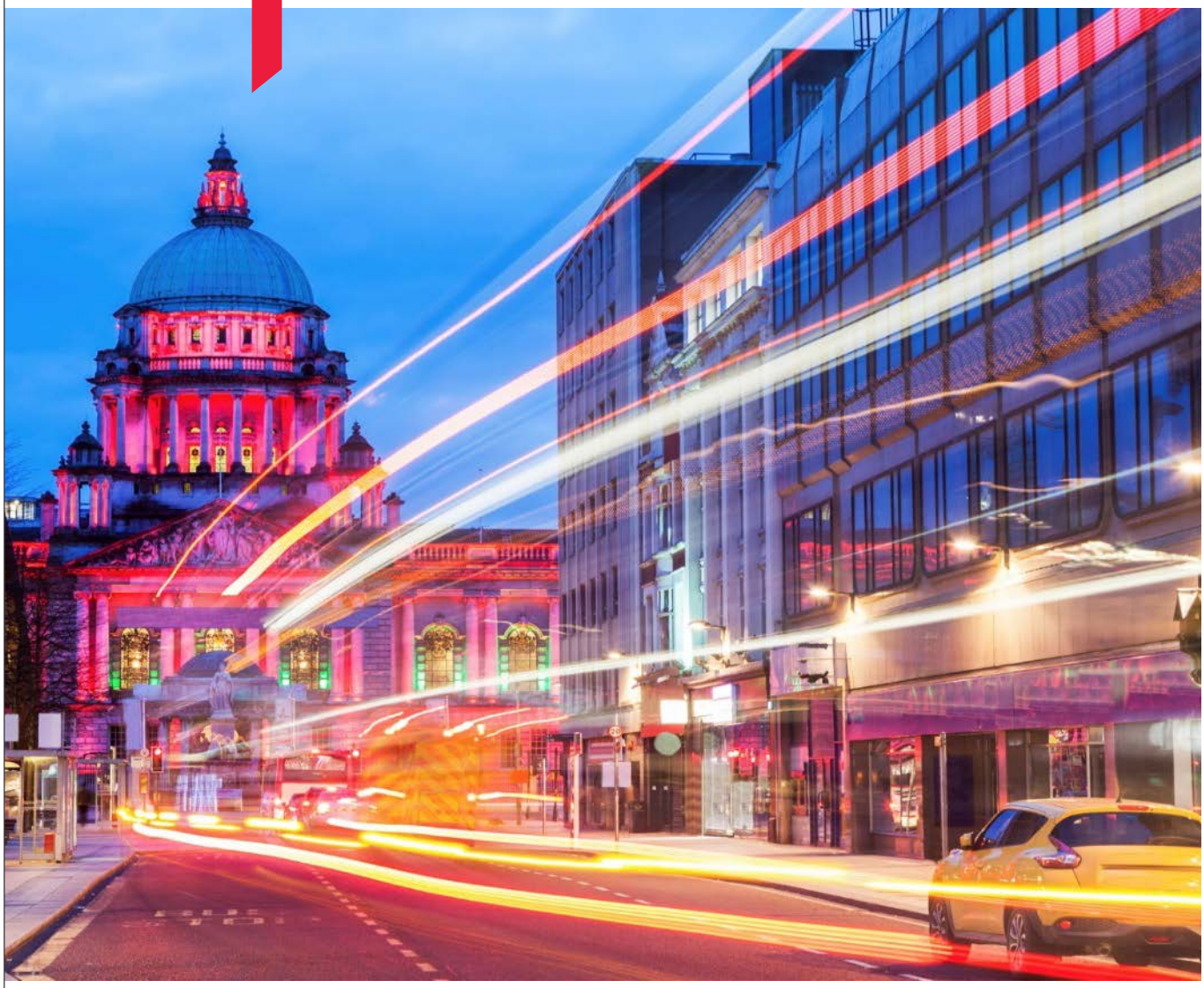

MALDON DISTRICT COUNCIL

INTERNAL AUDIT REPORT - FINAL

IT DISASTER RECOVERY
FEBRUARY 2020

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Limited	Moderate

IDEAS | PEOPLE | TRUST

BDO

DISTRIBUTION	
Annette Cardy	Resources Specialist Services Manager
Grant Hulley	Senior ICT Specialist

REPORT STATUS LIST	
Auditor	Antony Hadjirousos, Internal Auditor
Dates work performed	22 October 2019 – 13 November 2019
Draft report issued	20 November 2019
Final report issued	06 February 2020

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)

Design	Limited	System of internal controls is weakened with system objectives at risk of not being achieved
Effectiveness	Moderate	Evidence of non-compliance with some controls that may put some of the system objectives at risk

SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I)

High	1
Medium	3
Low	0

TOTAL NUMBER OF RECOMMENDATIONS: 4

BACKGROUND:

The services provided by the Council are dependent on the availability of Information Technology (IT) hardware and systems as well as the IT infrastructure that underpins them. Any disruption to the availability of these IT systems could result in the Council being unable to provide these services to the general public, which could result in financial and reputational losses.

Effective IT disaster recovery planning is therefore essential to ensuring that the Council is able to respond to system failures in the event of a major incident or disaster, in order to maintain operations of all critical systems. The Council's Information and Communication Technology (ICT) Department is responsible for managing the Council's disaster recovery arrangements and primary responsibility has been assigned to the Senior ICT specialist.

The purpose of this audit was to provide assurance that there are adequate arrangements in place to recover the Council's IT services, hardware and infrastructure in the event of a disaster.

GOOD PRACTICE:

Good practice was evidenced in the following areas:

- A business impact assessment has been performed for the loss of the Council's IT services, which includes an assessment of the potential impact on all major Council functions
- There is an ICT Business Continuity Plan in place, which defines the procedures for ensuring the continuity of the IT services in the event of an incident
- The roles and responsibilities of members of staff in the event of a disaster have been defined and communicated to all members of staff
- The Council has documented its backup arrangements and defined the procedures for restoring the backups as and when required.

KEY FINDINGS:

We identified the following areas of improvement:

- There are no arrangements in place for testing the Council's IT disaster recovery arrangements on a routine basis nor is there a defined schedule for testing backups for recoverability (**Finding 1 – High**)
- The Council has not performed a risk assessment of critical IT systems, applications and services being unavailable (**Finding 2 – Medium**)
- There is not a complete record of the Council's recovery time and point objectives for its critical IT infrastructure and systems (**Finding 3 – Medium**)
- The Council's IT Disaster Recovery Plan has not been finalised, approved and communicated to members of staff (**Finding 4 – Medium**).

CONCLUSION:

Based on our review we have raised one high and three medium level recommendations to improve the Council's IT disaster recovery arrangements.

Effective IT disaster recovery arrangements would enable the prioritisation of work to recover affected services in the event of a disaster and identify the key contacts, resources and processes required to return to stability of operations. Whilst the Council has taken action to ensure the continuity of elements of its critical IT systems and has informal arrangements in place to recover them in the event of a disaster, it does not have a defined recovery plan in place to support the recovery of the ICT service in line with its operational requirements. This could significantly disrupt the Council's ability to provide its critical services to the public.

Consequently, we conclude limited assurance over the design of the Council's IT disaster recovery arrangements and moderate assurance over their operational effectiveness.

DETAILED FINDINGS

RISK: THE RECOVERY ARRANGEMENTS ARE NOT TESTED ON A ROUTINE BASIS

Ref	Significance	Finding
1	High	Insufficient testing of the Council's backup and recovery arrangements It was observed during our fieldwork that the Council has not conducted a formal test of its IT disaster recovery arrangements nor has it established a requirement to test the arrangements on a routine basis. We found that whilst aspects of the Council's disaster recovery arrangements have been tested in May 2018, the Council has not fully assessed its ability to recover critical IT systems in the event of a disaster. Furthermore, there is not a defined schedule in place for testing backups for recovery on a routine basis. Not performing routine tests of the Council's disaster recovery arrangements, including testing backups for recoverability, increases the risk that they will not be sufficient to recover the Council's IT services in the event of a disaster.

RECOMMENDATION:

Management should conduct a formally documented test of the Council's IT disaster recovery arrangements and should establish a requirement to test the arrangements on a routine basis.

The results of the tests should be reported to Senior Management and any issues identified should be resolved in a timely manner.

Furthermore, management should put in place a defined schedule for testing backups for recoverability on a routine basis.

MANAGEMENT RESPONSE:

The council will now be running a planned testing plan every 6 months, this testing plan has now been finalised and is ready to be run. It includes testing of the network and services for core functionality. First test will be run 29th Feb / 1st March. Findings and an action plan following this test will be provided to the Resources Manager and to ensure all issues addressed by 31 March 2020.

Responsible Officer: Grant Hulley, Senior ICT Specialist

Implementation Date: 31st March 2020

RISK: THE IMPACT OF AN IT DISASTER ON THE COUNCIL HAS NOT BEEN ADEQUATELY ASSESSED		
Ref	Significance	Finding
2	Medium	Threats to the availability of the ICT service have not been assessed We observed during our fieldwork that the Council has not assessed the risk of the ICT service being unavailable. We found that whilst the Council has adequately assessed the business impact of the loss of its ICT services, it has not assessed the likelihood and impact of its critical IT systems and applications being unavailable nor has it undertaken a risk assessment to identify and assess the threats to the provision of the ICT service. The absence of a risk assessment increases the risk that the Council's resiliency and recovery arrangements will not be sufficient in the event of a disaster.

RECOMMENDATION:

Management should identify, assess and record the threats to the continuity of the Council's ICT service. Where appropriate, mitigating actions should be recorded and reviewed for efficacy on a routine basis.

Furthermore, management should assess the likelihood and impact of the Council's critical IT systems and applications being unavailable.

The assessments should be reviewed on a periodic basis or following a significant change to the Council's operations.

MANAGEMENT RESPONSE:

The risk assessment has now been updated to now include likelihood of loss of function / business impact this includes age, warranty, server cover

Responsible Officer: Grant Hulley, Senior ICT Specialist

Implementation Date: Completed.

RISK: THE RECOVERY OBJECTIVES ARE NOT ALIGEND TO THE COUNCIL'S CONTINUITY REQUIREMENTS		
Ref	Significance	Finding
3	Medium	The Council's recovery objectives have not been defined It was observed during our testing that the Council does not have a complete record of the Recovery Time Objectives (RTO) and the Recovery Point Objectives (RPO) for its critical IT infrastructure and systems. We found that whilst the Council has a server recovery plan in place, which includes the recovery time and point objectives for some systems, the plan has not been completed for all of the Council's critical systems and services, including the primary systems for Finance, Planning Services and Environmental Health Services. It was also observed that the Council has not determined the RTO and RPO for its IT infrastructure. This includes the hardware, software and all network components required for the Council's IT environment, which hosts the servers, systems and services provided by ICT. Furthermore, the Council has not included the time taken to recover the supporting IT infrastructure in determining IT system RTO. The absence of defined RTO and RPO increases the risk of the Council's critical services being disrupted when the IT systems that underpin them are unavailable.

RECOMMENDATION:

Management, in conjunction with appropriate stakeholders from across the Council, should determine the RTO and RPO for the Council's IT infrastructure and remaining IT systems that underpin the Council's critical services. Management should then use the defined objectives to revise the recovery prioritisation for systems and services in the event of a disaster.

The recovery objectives should be reviewed on a routine basis or following a significant change to the Council's operations.

Furthermore, the Council should review the procedures that support the recovery of its IT systems on a routine basis, to ensure that backup processes are sufficient to achieve the Council's expectations for the recovery of data in the event of a disaster.

MANAGEMENT RESPONSE:

The Recovery times list will be updated to include the new infrastructure hardware and servers. A column has been added to include infrastructure recovery time (this includes physical and virtual servers**.**

Responsible Officer: Grant Hulley, Senior ICT Specialist

Implementation Date: 31st March 2020

RISK: THERE ARE NOT DOCUMENTED PROCEDURES IN PLACE TO RECOVER CRITICAL IT INFRASTRUCTURE, HARDWARE OR SYSTEMS IN THE EVENT OF AN INCIDENT		
Ref	Significance	Finding
4	Medium	Absence of a defined IT disaster recovery plan It was observed during our fieldwork that the Council's IT disaster recovery arrangements have not been adequately defined. Whilst the Council has a draft IT Disaster Recovery Plan in place, the plan has not been finalised and approved and we found that it does not record: • The IT resources that would be required to support the Council's operations and how they would be obtained in the event of a disaster • The technical procedures for recovering critical IT infrastructure, systems and services in the event of a disaster • The procedures for returning to business as usual following the invocation of the plan. The absence of a defined IT disaster recovery plan increases the risk of the Council being unable to recover its IT systems that are required to provide its critical services.

RECOMMENDATION:

Management should review and, where necessary update the Council's IT Disaster Recovery Plan so that it includes, but is not limited to:

- The IT resources that are required in the event of a disaster and the procedures for obtaining them following the invocation of the plan
- The technical procedures for recovering critical IT infrastructure, systems and services in the event of a disaster
- The procedures for returning to business as usual.

The plan should be approved and communicated to all members of staff and should be stored so as to be easily accessible in the event of a disaster.

MANAGEMENT RESPONSE:

A list of IT resources has now been added to the DR plan with contact and priority details for staff required during the DR. The addition of an IT guide is also now been written to be included with the DR, this will contain step by steps on the recovery process.

This will be approved by the Resources Manager and communicated and shared with all staff by 31st March 2020. A link to the plan will be added to the Corporate Sharepoint page accessible for all

Responsible Officer: Grant Hulley, Senior ICT Specialist

Implementation Date: 31st March 2020

STAFF INTERVIEWED

BDO LLP APPRECIATES THE TIME PROVIDED BY ALL THE INDIVIDUALS INVOLVED IN THIS REVIEW AND WOULD LIKE TO THANK THEM FOR THEIR ASSISTANCE AND COOPERATION.

Annette Cardy	Resources Specialist Services Manager
Grant Hulley	Senior ICT Specialist

APPENDIX I – DEFINITIONS

LEVEL OF ASSURANCE	DESIGN OF INTERNAL CONTROL FRAMEWORK		OPERATIONAL EFFECTIVENESS OF CONTROLS	
	FINDINGS FROM REVIEW	DESIGN OPINION	FINDINGS FROM REVIEW	EFFECTIVENESS OPINION
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

RECOMMENDATION SIGNIFICANCE	
High	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

APPENDIX II - TERMS OF REFERENCE

PURPOSE OF REVIEW:

The purpose of this audit is to provide assurance that the Council has adequate arrangements in place to recover its IT services, hardware and infrastructure in the event of a disaster.

KEY RISKS:

Based upon the risk assessment undertaken during the development of the internal audit operational plan, through discussions with management, and our collective audit knowledge and understanding the key risks associated with the area under review are:

- The impact of an IT disaster on the Council has not been adequately assessed
- The recovery objectives are not aligned to the Council's continuity requirements
- There are not documented procedures in place to recover critical IT infrastructure, hardware or systems in the event of an incident
- Roles and responsibilities for managing the response to a disaster have not been defined
- There are not adequate backup and recovery procedures in place
- The recovery arrangements are not tested on a routine basis.

SCOPE OF REVIEW:

The following areas will be covered as part of this review:

- Evidence that the risk and impact of a disaster has been assessed
- Determine whether recovery time and point objectives have been defined and whether the priorities of the Council are reflected in its IT disaster recovery arrangements
- Review the IT Disaster Recovery plan to identify whether it contains the information necessary to recover systems and services in the event of a disaster
- Determine whether roles and responsibilities associated with disaster recovery have been defined
- Assess the arrangements for backing up and recovering critical IT systems and services
- Determine the frequency with which the IT disaster recovery arrangements are tested and the adequacy of the testing performed.

However, Internal Audit will bring to the attention of management any points relating to other areas that come to their attention during the course of the audit. We assume for the purposes of estimating the number of days of audit work that there is one control environment, and that we will be providing assurance over controls in this environment. If this is not the case, our estimate of audit days may not be accurate.

APPROACH:

Our approach will be to conduct interviews to establish the controls in operation for each of our areas of audit work. We will then seek documentary evidence that these controls are designed as described. We will evaluate these controls to identify whether they adequately address the risks.

We will seek to gain evidence of the satisfactory operation of the controls to verify the effectiveness of the control through use of a range of tools and techniques.

FOR MORE INFORMATION:

Greg Rubins

Greg.Rubins@bdo.co.uk