MALDON DISTRICT COUNCIL

INTERNAL AUDIT REPORT – DRAFT

IT DISASTER RECOVERY AND BUSINESS CONTINUITY
MAY 2025

Design Opinion	● Substantial
Effectiveness Opinion	● Substantial

IDEAS | PEOPLE | TRUST

CONTENTS

DISTRIBUTION	
Ben Cookson	Interim Chief Finance Officer
Annette Cardy	Assistant Director - Resources
Grant Hulley	Lead Specialist: ICT Resources Directorate

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.

REPORT STATUS	
Auditors:	Aaron Winter - Partner Andrew Billingham - Internal Audit Manager Antony Hadjirousos - IT Audit Senior Manager
Dates work performed:	25 November 2024 - 20 January 2025
Draft report issued:	14 February 2025
Management responses received:	15 May 2025
Final report issued:	15 May 2025

EXECUTIVE SUMMARY

Control Design	● Substantial	Control Effectiveness	● Substantial
Recommendations	🟥 0 🟧 0 🟩 1		

SCOPE

BACKGROUND

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

Furthermore, cyber security incidents can have significant impact on the business operations of any organisation and every effort should be made to both prevent and minimise their impact. With an increasing reliance on IT in local government, all councils are required to ensure that IT systems are appropriately protected to prevent any significant disruption and can be recovered quickly in the event of a disaster to limit any impact on customer services.

The Civil Contingencies Act 2004 (the Act) delivers a single framework for civil protection in the UK. The Act establishes a clear set of roles and responsibilities for those involved in emergency preparation and response at a local level. The Act identifies Local Authorities as “category one” responders, which means that they are subject to the full set of civil protection duties.

Effective IT disaster recovery planning is therefore essential to ensuring that the Council can respond to system failures in the event of a major incident or disaster to maintain operations of all critical systems.

Internal Audit completed an IT Disaster Recovery audit in 2019/20, which provided limited assurance over the design of the Council’s IT disaster recovery controls and moderate assurance over their operational effectiveness. The audit raised one high and three medium priority recommendations, which related to the absence of documented, finalised and sufficiently tested IT disaster recovery arrangements, including the lack of defined recovery objectives, business impact and risk assessments.

PURPOSE

The purpose of the audit was 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, including whether the recommendations raised as part of the 2019/20 have been implemented.

AREAS REVIEWED

The following areas were covered as part of this review:

- Determine whether the Council has identified its critical business services and prioritised them as part of its disaster recovery planning activities, including whether the Council has identified, assessed and documented the risks of the loss of its IT systems and services.
- Determine whether there are documented procedures in place to recover critical IT infrastructure, hardware, or systems in the event of an incident, including whether the Council has a defined IT Disaster Recovery Plan and IT Business Continuity Plan in place, whether the procedures for recovering critical systems and services have been

documented and whether roles and responsibilities for members of staff have been defined and communicated.

- Determine whether Recovery Time and Point Objectives (RTOs and RPOs) have been defined and whether they are aligned to the Council's continuity requirements, and whether there are defined backup and recovery arrangements in place for critical IT systems and services.
- Determine whether there are arrangements in place for testing the Council's disaster recovery arrangements on a routine basis and providing training to staff.

AREAS OF STRENGTH

During our review, we identified the following areas of good practice:

- The Council has identified, assessed, and maintains a listing of its high-risk, medium-risk and low-risk functions, which was found to be regularly reviewed and kept up to date. The register, which subsequently forms the basis for business continuity and disaster recovery planning activities, assesses the business impact of the unavailability of the functions in terms of finance, operations, reputation, people, major projects and legal and regulatory. The listing was last reviewed in March 2024, and is due for further review in March 2025, and is accompanied by an identification of critical IT systems and their suppliers, along with their day-to-day and disaster recovery dependency levels.
- Risks to the continuity and availability of the IT Service have also been identified and assessed as part of the Council's IT Risk Register and Data Security Risk Register. Review of the registers found them to include, for each risk, overall risk scores (including a breakdown between likelihood and impact), risk owner details and an overview of existing controls, an assessment of the strength of the current control environment and a mitigated risk score.
- The Council's IT network Is set up on high availability and there is live failover between four hosts allowing for instant restore in the event of an incident. There are documented technical standard operating procedures in place for performing full backups through the Veeam solution, which would restore the availability and operation of the network, and critical systems and services, in line with the established recovery objectives.
- The Council has a Business Continuity Strategy in place, which was formally approved and adopted in April 2024 and provides a strategic approach to key aspects of business continuity management and a framework for maintaining the Council's ability to deliver critical service functions. Review of the Strategy found it to include the procedures for the invocation of the Council-wide business continuity plans, the roles and responsibilities of members of staff, requirements relating to business continuity risk identification and business impact analysis, and the key resilience and business continuity procedures, including those for the IT Service.
- In addition to the Business Continuity Strategy and the Council-wide Business Continuity Plan, there are also defined IT Business Continuity and IT Disaster Recovery Plans in place that specifically define the procedures relating to the continuity and recovery of the IT Service. These were found to be up to data and in line with their annual review cycle requirements, and were found to include, but not being limited to, plan invocation procedures, backup and recovery procedures, example recovery scenarios and the arrangements for restoring from backups, recovery objectives, and key contact details, including supplier and third-party partner information.

- There are arrangements in place for regularly testing the Council's IT disaster recovery and business continuity arrangements, which include system-wide testing twice per year, and an annual tabletop exercise that consists of a discussion-based session where team members review a disaster scenario and how they would respond. The most recent testing was completed in July 2024, and through our review of attendance logs, training slides, and testing notes, we confirmed that key stakeholders and members of staff have been provided with relevant training for their role. Furthermore, backups are tested for recoverability on a regular basis, in line with the Council's backup testing schedule.

AREAS OF CONCERN

During our review, the following area of improvement was identified:

- Whilst there are defined and formally documented RTOs and RPOs in place, the Council has not completed a full assessment of its ability to achieve these in the event of an incident or disaster **(Finding 1 - Low).**

CONCLUSION

We have raised one low priority recommendation to further strengthen the Council's IT disaster recovery and business continuity controls and enhance its IT network resilience and service availability in the event of an incident or disaster.

Control Design

The Council has identified, assessed, and prioritised its critical IT systems and services based on robust business impact and risk assessments and has defined recovery objectives based on this prioritisation and in line with corporate objectives. There are defined business continuity and disaster recovery plans in place, which include procedures and roles and responsibilities of members of staff, as well as technical standard operating procedures for the back-up and full recovery of critical IT systems and services in the event of an incident or disaster. Therefore, we concluded 'Substantial' assurance over the design of the Council's IT business continuity and disaster recovery controls.

Control Effectiveness

The Council has appropriate, and regularly tested, backup and recovery arrangements in place, which alongside the regular testing of the Council's IT disaster recovery and business continuity procedures and the training provided to members of staff would help to ensure that the procedures will be effectively applied in the event of an incident or disaster. Furthermore, recovery objectives have been defined for each individual system or service, and while there has not been a complete assessment of the feasibility of these objectives, the Council has a defined schedule of tests in place that includes a full assessment of all IT systems covering complete physical hardware restores, entire virtual machine restores, and full data restores. Consequently, we also concluded 'Substantial' assurance over the operational effectiveness of the Council's IT business continuity and disaster recovery controls.

The scope of our review is limited to the areas documented under the scope and approach section of the agreed Terms of Reference (see Appendix II). Our work is therefore designed to provide an assessment of the IT disaster recovery and business continuity arrangements that are in place, and the controls assessed support a strong foundation that is informing the opinion provided, but we cannot provide absolute assurance in the event of an incident.

DETAILED FINDINGS

1 Recovery Time and Point Objectives (RTOs and RPOs)

TOR Risk:	If the Council’s data recovery objectives have not been defined and are not aligned to the Council’s business continuity requirements, there is a risk that service continuity and restoring in the event of a disaster will not be in line with the expectations of the Council’s and the various Service Areas if the recovery of critical systems or infrastructure is not prioritised.
Significance	● Low

FINDING

Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) are critical components of the Council’s IT disaster recovery and business continuity planning. The RPOs define the maximum acceptable amount of data loss measured in time, while the RTOs set the target time for the recovery of each system after a disruption. It is therefore essential that these are defined, thoroughly assessed and regularly reviewed to ensure that recovery and continuity procedures will be sufficient in the event of an incident or disaster.

Whilst the Council has defined the RTOs and RPOs for its critical IT systems and services, we found that there has not been a formally documented assessment of the Council’s ability to achieve these in the event of a critical incident or disaster. However, whilst this assessment has not been formally documented, we confirmed through our testing and discussions with Management that there is a full disaster recovery and business continuity testing schedule in place, which includes a full assessment of all ICT systems that covers complete physical hardware restores, entire virtual machine restores, and full operating system and data restores.

Where recovery objectives are not regularly or sufficiently tested, including performing a full assessment of the Council’s ability to achieve these in the event of a critical incident or disaster, there is an increased risk that recovery strategies may not be effective during an actual critical incident or disaster, leading to prolonged downtime and potential data loss. This can result in financial losses, reputational damage and non-compliance with regulatory requirements.

RECOMMENDATION

Management should perform, and formally document, a thorough assessment of the Council’s ability to achieve the defined recovery objectives in the event of a critical incident or disaster. Following the assessment, the recovery objectives should be reviewed and, where necessary, updated, and arrangements should be put in place for reviewing them on a routine basis, as well as for testing the Council’s ability to achieve them.

Furthermore, the procedures that support the recovery of the Council’s IT systems and services should also be reviewed and tested 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

We acknowledge the importance of thoroughly assessing and formally documenting our ability to achieve the defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) in the event of a critical incident or disaster.

We are committed to enhancing our disaster recovery (DR) and business continuity planning (BCP). As part of this commitment, we will ensure that a comprehensive assessment of our current recovery capabilities is conducted and documented, whilst DR and BCP testing is run for ICT at a minimum of every six months, A full council wide DR and BCP scenario will be arranged and scheduled to run at least once per annum. This assessment will help us identify any potential gaps and areas for improvement in our recovery stages. Following this testing, we will establish a routine schedule for reviewing and updating our recovery objectives to ensure they remain aligned with our changing systems and business continuity requirements.

These scheduled scenarios will be documented and reported to senior management for review upon completion, to define any key RTOs.

Responsible Officer:	Grant C Hulley
Implementation Date:	December 2025

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

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 potential key risks associated with the area under review are:

- Risk 1: If the Council has not identified its critical business services and prioritised them as part of its disaster recovery planning activities, there is a risk that business continuity and disaster recovery procedures may not be adequate to ensure service continuity and provision in the event of a disaster, which could prevent the Council from providing services to the public.
- Risk 2: If the Council has not documented the formal procedures required to recover the critical IT infrastructure, hardware, or systems in the event of a cyber incident, there is a risk that it will be unable to operate in the event of a disaster if these critical systems cannot be promptly recovered.
- Risk 3: If the Council's data recovery objectives have not been defined and are not aligned to the Council's business continuity requirements, there is a risk that service continuity and restoring in the event of a disaster will not be in line with the expectations of the Council's and the various Service Areas if the recovery of critical systems or infrastructure is not prioritised.
- Risk 4: If the Council does not have effective arrangements in place for testing the Trust's disaster recovery arrangements on a routine basis and staff are not adequately trained in this area, there is a risk that the disaster recovery and business continuity procedures may not be sufficient in the event of a disaster, which could prevent the Council from operating and providing services to the public.

SCOPE & APPROACH

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

- **Business Impact and Risk Assessments -** We will determine whether the Council has identified its critical business services and prioritised them as part of its disaster recovery planning activities (Risk 1):
  - Critical business services have been identified and assessed through an appropriate business impact analysis.
  - The Council has identified, assessed and documented the risks of the loss of its IT systems and services.
- **Disaster Recovery Planning -** We will determine whether there are documented procedures in place to recover critical IT infrastructure, hardware, or systems in the event of an incident (Risk 2):
  - The Council has a defined IT Disaster Recovery Plan and IT Business Continuity Plan in place, which can be accessed in the event of an incident.
  - The procedures for recovering critical IT systems and services have been documented.
  - Roles and responsibilities for members of staff involved in the Council's disaster recovery arrangements have been defined and communicated.
- **Recovery Objectives -** We will determine whether recovery objectives have been defined and whether they are aligned to the Council's continuity requirements (Risk 3):

  - There are defined recovery time and point objectives in place, and they are reviewed on a routine basis.
  - There are defined backup and recovery arrangements in place for critical IT systems and services.
- **Disaster Recovery Testing and Training -** We will determine whether there are arrangements in place for testing the Council's disaster recovery arrangements on a routine basis and providing training to staff (Risk 4):
  - The Council's IT disaster recovery arrangements are tested on a routine basis and lessons are learned from the tests undertaken.
  - Backups are tested for recoverability on a routine basis.
  - Key members of staff involved in the Council's disaster recovery processes have been adequately trained.

The scope of the review is limited to the areas documented under the scope and approach. All other areas are considered outside of the scope of this review. However, Internal Audit will bring to the attention of management any points relating to other areas that come to their attention during 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.

In delivering this review BDO may need to observe and test confidential or personal identifiable data to ascertain the effective operation of controls in place. The organisation shall only provide the Shared Personal Data to BDO using secure methods as agreed between the parties. BDO will utilise the data in line with the Data Protection Act 2018 (DPA 2018), and the UK General Data Protection Regulation (UK GDPR) and shall only share Personal Data on an anonymised basis and only where necessary.

FOR MORE INFORMATION:

Aaron Winter

Aaron.Winter@bdo.co.uk

The matters raised in this report are only those which came to our attention during the course of our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO Member Firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.