Maldon District Council

Internal Audit Report - Final

IT GOVERNANCE

APRIL 2026

Design Opinion	Moderate
Effectiveness Opinion	Moderate

IDEAS | PEOPLE | TRUST

CONTENTS

DISTRIBUTION	
Ben Jay	Director of Finance and s151 Officer
Grant Hulley	Head of ICT and Digital Strategy & Improvement 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 – Senior IT Audit Manager
Dates work performed:	4 December 2025 – 30 March 2026
Draft report issued:	1 April 2026
Management Response Received:	29 April 2026
Final report issued:	30 April 2026

Executive Summary

Design Opinion	Moderate	Effectiveness Opinion	Moderate

Recommendations	0	2	0

SCOPE

Background

- Maldon District Council (the Council), like all other public sector organisations, is increasingly reliant on digital services, data and Information Technology (IT) to deliver statutory obligations, citizen-facing services and internal operations. In recent years, demand for digital transformation has accelerated due to service pressures, hybrid working models, security expectations and the need for resilient infrastructure.
- Effective IT governance is therefore essential to ensure that technology decisions are aligned to organisational objectives, risks are managed proactively, public funds are used efficiently, and cyber resilience is maintained.
- As the Council continues to modernise key systems, expand digital platforms and manage a complex portfolio of IT projects and suppliers, robust governance arrangements are critical in maintaining accountability, control and transparency. Weaknesses in governance structures, risk oversight, security controls or project delivery could impact service availability, financial stewardship, data protection and public trust.

Purpose

- The purpose of the audit was to provide assurance over the adequacy and effectiveness of the Council's IT governance arrangements. This included the Council's IT governance framework, decision-making structures, oversight mechanisms and supporting processes that are in place to enable the delivery of strategic priorities, manage risks and safeguard information assets.

Areas reviewed

- **Governance Structure and Strategic Alignment**: We reviewed the Council's IT strategy for alignment to corporate objectives, examined IT governance forums and their documentation, and assessed the clarity of ICT leadership roles and responsibilities.
- **IT Risk Management and Regulatory Compliance**: We reviewed the IT and digital risk registers, assessed procedures for regulatory and security compliance, and examined incident logs, root cause analyses and lessons learned.
- **Project and Change Portfolio Governance**: We reviewed the IT project portfolio and supporting documentation and examined change control processes and post-implementation reviews for the capture of benefits and lessons learned.
- **Information Security Oversight and Cyber Resilience**: We reviewed the Council's information security policies and governance documentation, assessed cyber and information governance training completion and awareness activity, and examined access governance arrangements for starters, movers, leavers and privileged accounts.

- **IT Performance Management and Resource Capability**: We reviewed ICT performance reporting mechanisms, assessed ICT workforce skills and capacity arrangements, examined vendor and contract management controls, and reviewed resource risk and succession planning arrangements.

AREAS OF STRENGTH

- The Council's ICT Strategy explicitly references the Corporate Plan's themes (supporting communities, investing in the district, growing the economy, protecting the environment and delivering good quality services) and sets out corresponding ICT priorities such as security management, cloud migration, digital process optimisation and data-driven decision making. ICT is therefore not being developed in isolation but is tightly connected to corporate aims, with investment and transformation projects embedded into the Technology Roadmap across 2024 to 2027.
- The Council maintains a portfolio of information security policies that are up to date, clearly formatted and accessible internally. These include the Information Security Policy, Acceptable Use Policy, Cyber Security Policy and Using Email & Digital Communications guidance, each with defined version control, defined review cycles, and wide circulation to staff. The policies provide detailed guidance on responsibilities, data handling, legal obligations, password and device usage, monitoring provisions, confidentiality requirements and secure communications.
- Cyber training completion rates are high across several service areas, with many users completing all assigned modules. Training has been rolled out widely across Members and staff, reflecting broad organisational coverage, and is delivered systematically with structured modules and defined completion tracking for each user. Cyber training obligations are also embedded within multiple governance documents, including the Cyber Security Policy and Acceptable Use Policy, reinforcing a strong institutional commitment to building cyber awareness.
- The Technology Roadmap provides a detailed breakdown of multi-year ICT programmes, including Dynamics rollout, ArcGIS integration, Azure migration, Windows 365 development and Intune deployment. Each initiative includes defined timelines spanning 2024 to 2027, reflecting a planned and sequenced approach to deploying major systems and infrastructure changes. Alongside system modernisation, the roadmap accounts for BAU activities and resilience improvements, demonstrating that transformation is being balanced with operational continuity.
- The Council operates structured project governance, including a central PMO, highlight reporting, scheduled project boards and well-defined agenda items. Project board meetings include updates from multiple project managers, cross-service engagement, risk and issue discussions, and follow-up actions assigned to named officers, demonstrating an organised and repeatable governance process for monitoring programmes and projects.
- The ICT Risk Register provides detailed descriptions of ICT operational risks, including infrastructure failures, cyber security exposures, cloud service risks, data privacy concerns, ransomware, supplier assurance issues and behavioural risks. Each risk includes clear impact and likelihood scoring, mitigating controls, risk direction and responsibility assignments, with many showing active control environments such as backups, MFA, dark-web scanning, SOC monitoring and failover infrastructure.

- Across the Corporate Plan and ICT Strategy, the Council sets out clear commitments to cloud-based platforms, hybrid working models, collaborative technologies and digital access for residents. Initiatives such as the shift to Microsoft Azure, use of Dynamics for process automation, adoption of Power BI for reporting and the integration of IoT and data-centric systems all indicate a strong orientation toward modern digital tools. Remote working enablement, multi-device access and flexible working practices are referenced throughout strategic documents, demonstrating that digital modernisation extends beyond infrastructure to working culture and service design.
- ICT is deeply integrated into change programmes across the organisation. Project board meetings show ICT involvement in system development, access control upgrades, Local Development Plan processes, digital replacements for manual systems and process improvement initiatives, with ICT dependencies, resource considerations and system integration challenges routinely discussed in governance forums. Standardised reporting, escalation routes and iterative development cycles demonstrate that change management is a coordinated cross-service activity in which ICT plays a formal and active role.

AREAS OF CONCERN

- The Council faces ICT capacity limitations without a formal workforce, skills or succession planning framework to mitigate the resulting risks **(Finding 1 - Medium)**
- Despite a strong suite of cyber policies, training and controls, phishing simulation data shows a persistent cohort of high-risk users whose behaviour continues to expose the organisation to cyber threats **(Finding 2 - Medium).**

CONCLUSION

We conclude Moderate assurance over both the design and operational effectiveness of the Council's IT governance arrangements and controls. The Council has in place a broad and established framework of ICT strategies, policies, risk management processes, security controls and project governance structures; however, further development is required in specific aspects of the control environment to strengthen overall maturity and alignment with good practice. The two findings identified, relating to ICT workforce and skills planning, and the management of persistent user-level cyber risk, affect both the design of controls and their practical application.

Control Design

- We have concluded Moderate assurance for control design due to identified gaps in the Council's ICT workforce and capability planning framework, and in the design of behaviour-focused cyber risk controls.
- Although the Council maintains a comprehensive ICT Strategy, Technology Roadmap and suite of information governance policies, the control framework does not currently include a formal ICT workforce plan, skills matrix, or succession model for key roles. In addition, while cyber training and phishing simulations are well established, there is no structured escalation pathway or defined intervention process for individuals repeatedly demonstrating high-risk cyber behaviour.
- These gaps limit the completeness and maturity of the design, despite strong strategic foundations and well-developed documentation in other areas.

Control Effectiveness

- We have concluded Moderate assurance for control effectiveness, as testing confirmed that many ICT governance activities are operating effectively in practice, such as cyber training delivery, use of project governance structures, and active monitoring of ICT risks.
- However, operational weaknesses remain in addressing persistent user-level cyber vulnerabilities and in managing ICT capacity constraints, which affect the timely and consistent execution of ICT responsibilities. While controls are functioning across most areas, these issues demonstrate that operational practices do not yet fully align with the intended governance framework.
- As a result, while day-to-day ICT processes are generally effective, further strengthening is needed to achieve greater consistency, resilience and behavioural control.

Detailed Findings

1 ICT Capacity Constraints and Absence of Formal Workforce and Succession Planning

TOR Risk:	Insufficient skills, vendor performance gaps and weak service measurement may reduce the ability of the IT Service to support wider Council services
Significance	Medium

FINDING

Issue

The ICT Strategy notes that the ICT team operates with limited resources, and project board records further highlight delays caused by ICT capacity constraints and specialist skill shortages.

More specifically, the ICT Strategy also sets out a future requirement for broadening ICT capability in areas such as cloud management, project delivery, cyber security, data analytics and process automation, but no corresponding workforce plan or skills matrix is in place to demonstrate how these requirements will be met.

Similarly, although the ICT Risk Register documents "ICT skills & capacity" as a recognised risk, we found that the following are not in place:

- Any formal ICT workforce plan or capacity model aligned to the Technology Roadmap
- A skills matrix or competency assessment to identify capability gaps
- A succession plan for key technical leadership roles
- Formal resourcing forecasts for major digital transformation programmes.

Root cause

ICT workforce planning activities have not been formally developed or documented, likely due to competing operational priorities and limited capacity within the ICT team itself.

Implications

The Council remains at risk of project delays, service interruptions, increased reliance on single points of failure and an inability to meet the demands of digital transformation. Over time, this may result in higher costs, lower service quality and difficulty sustaining ICT capabilities.

RECOMMENDATION

i. The Council should introduce a structured ICT workforce and capability planning process. This should include, but not be limited to:

- A formal ICT workforce strategy aligned to the Technology Roadmap and organisational priorities
- A skills matrix and gap analysis covering all key ICT roles.
- A defined resourcing model that considers ongoing operations, project delivery and emerging technology requirements.
- A succession plan for critical roles, with knowledge transfer activities embedded as standard.

MANAGEMENT RESPONSE

Following the completion of the phase 2 restructure, MDC ICT have opened four additional posts to build on the resources available within the ICT team. These posts are out for advertising as of April, with the intent to interview and then formally hire as of May / June

Responsible Officer:	i.	Grant C Hulley – Head of ICT and Digital Strategy & Improvement Directorate
Implementation Date:	i.	May 2026

2 Persistent User-Level Cyber Risk Despite Strong Cyber Governance Framework

TOR Risk:	Weak security governance could lead to data breaches, fraud or service outages, which could harm citizens and breach statutory obligations
Significance:	Medium

FINDING

Issue

The Council has implemented a robust and modern cyber governance environment, including defined policies, procedures and guidance that collectively set clear behavioural and technical security expectations, and Council-wide cyber training and regular phishing simulations through Boxphish, which is recognised good practice.

However, we found that while many users achieve 100% training completion, the simulation results highlight repeat click-through behaviour among several users, including staff and Members, across multiple simulation cycles. Some individuals recorded 4–5 clicks in a single 24-hour simulation series, indicating a heightened vulnerability to phishing attacks.

This persistent behavioural risk means that human-factor vulnerabilities remain a material exposure despite the Council's strong policy frameworks, technical safeguards (such as MFA and monitoring), and extensive training programme.

Root cause

Current training and simulation programmes do not sufficiently target repeat high-risk users with tailored interventions. Behavioural risk management processes are not yet mature enough to escalate or mitigate persistent user-level vulnerabilities.

Implications

The Council remains at continued risk of phishing-related compromise, including credential theft, data breaches, malware infection and system disruption. This risk is particularly sensitive given the Council's reliance on cloud technologies and the wide access privileges held by some high-risk users.

RECOMMENDATION

i. The Council should supplement its existing training and simulation activities with targeted, risk-based interventions for users who exhibit repeated high-risk behaviour. These interventions may include, but not be limited to:

- Mandatory one-to-one remedial training for repeat clickers
- Temporary restrictions or enhanced monitoring for high-risk accounts
- Scenario-based or role-specific training modules focusing on decision-making under pressure
- Escalation pathways for persistent non-compliance, particularly for users with privileged access or governance responsibilities.

Implementing a behaviourally-focused risk management programme will significantly reduce residual cyber exposure and strengthen the Council's cyber resilience.

MANAGEMENT RESPONSE

Maldon District Council (MDC) have implemented temporary restrictions on user accounts for repeat clickers or failed course learning, with an escalation path via SLT and staff disciplinarians in the event of multiple failures to pass cyber awareness courses.

Responsible Officer:	i.	Grant C Hulley – Head of ICT and Digital Strategy & Improvement Directorate
Implementation Date:	i.	April / May 2026

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	Several 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.	Several 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 (including those relevant to the IIA's Cyber Security Topical Requirement), are:

- **Risk 1**: IT strategy and governance roles may not align with the wider Council objectives, leading to poor prioritisation, inefficient resource allocation and failure to deliver statutory or essential services
- **Risk 2**: IT risks may not be identified or managed proactively, exposing the Council to service disruption and legal non-compliance
- **Risk 3**: Inconsistent project governance may cause delays, cost overruns and inefficient use of public funds, affecting wider service quality
- **Risk 4**: Weak security governance could lead to data breaches, fraud or service outages, which could harm citizens and breach statutory obligations
- **Risk 5**: Insufficient skills, vendor performance gaps and weak service measurement may reduce the ability of the IT Service to support wider Council services.

SCOPE & APPROACH

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

Governance Structure and Strategic Alignment (Risk 1):

- Reviewing the Council's IT strategy to determine whether it aligns with corporate objectives, service plans and strategic priorities
- Examining the governance forums responsible for IT decision-making by assessing their terms of reference, membership, meeting frequency and the quality of decision logs
- Assessing whether roles and responsibilities for IT leadership are clearly defined and understood across the organisation.

IT Risk Management and Regulatory Compliance (Risk 2):

- Evaluating the completeness and quality of IT and digital risk registers, including ownership, scoring and mitigation plans, and verifying the frequency and adequacy of risk monitoring and reporting to senior leadership
- Assessing procedures in place for ensuring compliance with regulations and security standards, such as the UK GDPR, PSN, Cyber Essential Plus and wider Local Government and NCSC guidance
- Analysing recent incident logs, root-cause analyses and lessons learned to assess whether the Council is effectively identifying, responding to, and preventing IT incidents.

Project and Change Portfolio Governance (Risk 3):

- Reviewing the Council's IT project portfolio register to assess prioritisation processes and the criteria used to approve new investments and whether business cases and project initiation documents are in place and include clear scopes, costs, benefits, dependencies and risk assessments

- Reviewing change control procedures and post-implementation review documentation to determine whether benefits realisation and lessons learned are captured and acted upon.

Information Security Oversight and Cyber Resilience (Risk 4):

- Reviewing information security policies, strategies and governance documentation to determine whether they are up to date, approved and communicated to members of staff
- Assessing completion rates for mandatory cyber and information governance training and, where applicable, reviewing the outcomes of phishing simulations and other campaigns for raising Cyber awareness
- Assessing whether access governance controls are in place for starters, movers and leavers to confirm that access is granted, amended or removed appropriately, as well as for the management of privileged user accounts.

IT Performance Management and Resource Capability (Risk 5):

- Reviewing performance reporting, including Service Level Agreements (SLAs) and Key Performance Indicators (KPIs) to assess whether the IT function is meeting agreed service standards
- Assessing the Council's IT workforce plan, skills matrix and capacity arrangements to determine whether resourcing is adequate to meet current and future demand
- Assessing whether there are vendor and contract management controls in place that include risk or issue escalation procedures
- Reviewing succession planning and resource risk assessments to determine whether the Council has effective plans in place for critical IT roles.

Sample sizes will be determined following the completion of our walkthroughs using our Internal Audit Methodology; for example, if a control is performed daily, we may select a sample of fifteen and if monthly a sample of two to three. Where possible, full population testing will be conducted utilising data analytics.

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 course of the audit.

A closing meeting will be held to discuss findings emerging from the review prior to issue of the draft report. Once the report and recommendations have been agreed following discussions with management, a summary of the findings will be presented to the Audit Committee]at its next meeting. 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.

Appendix III - Responsibilities and conformance

Management responsibilities

The Global Internal Audit Standards (GIAS) refer to the 'board' as 'the highest-level body charged with governance, such as a board of directors, an Audit Committee, a board of governors or trustees, or a group of elected officials or political appointees.' For the Council, 'the board' is the Performance, Governance and Audit Committee (PGAC) acting on behalf of the Council.

The PGAC is responsible for determining the scope of internal audit work, and for deciding the action to be taken on the outcome of our findings from our work.

The PGAC is responsible for ensuring the internal audit function has:

- The support of the Council's management team.
- Direct access and freedom to report to senior management, including the Chair of the PGAC.
- The AC is responsible for the establishment and proper operation of a system of internal control, including proper accounting records and other management information suitable for running the Council.

Internal controls covers the whole system of controls, financial and otherwise, established by the Council in order to carry on the business of the Council in an orderly and efficient manner, ensure adherence to management policies, safeguard the assets and secure as far as possible the completeness and accuracy of the records. The individual components of an internal control system are known as 'controls' or 'internal controls'.

The PGAC is responsible for risk management in the organisation, and for deciding the action to be taken on the outcome of any findings from our work. The identification of risks and the strategies put in place to deal with identified risks remain the sole responsibility of the Council.

Limitations

The scope of the review is limited to the areas documented under Appendix V - Terms of reference. All other areas are considered outside of the scope of this review.

Our work is inherently limited by the honest representation of those interviewed as part of the review. Our work and conclusion is subject to sampling risk, which means that our work may not be representative of the full population.

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness may not be relevant to future periods due to the risk that: the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or the degree of compliance with policies and procedures may deteriorate.

Conformance with the Global Internal Audit Standards in the UK Public Sector

This engagement has been conducted in accordance with Global Internal Audit Standards in the UK Public Sector, which encompass:

- The global Institute of Internal Auditors (IIA) *Global Internal Audit Standards* effective from January 2025
- The Internal Audit Standards Advisory Board (IASAB) *Application Note Global Internal Audit Standards in the UK Public Sector* effective from 1 April 2025.

FOR MORE INFORMATION:

Aaron Winter

Aaron.Winter@bdo.co.uk

Freedom of Information

In the event you are required to disclose any information contained in this report by virtue of the Freedom of Information Act 2000 ("the Act"), you must notify BDO LLP promptly prior to any disclosure. You agree to pay due regard to any representations which BDO LLP makes in connection with such disclosure, and you shall apply any relevant exemptions which may exist under the Act. If, following consultation with BDO LLP, you disclose this report in whole or in part, you shall ensure that any disclaimer which BDO LLP has included, or may subsequently wish to include, is reproduced in full in any copies.

Disclaimer

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

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.

The matters raised in this report are only those which came to our attention during 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.

www.bdo.co.uk