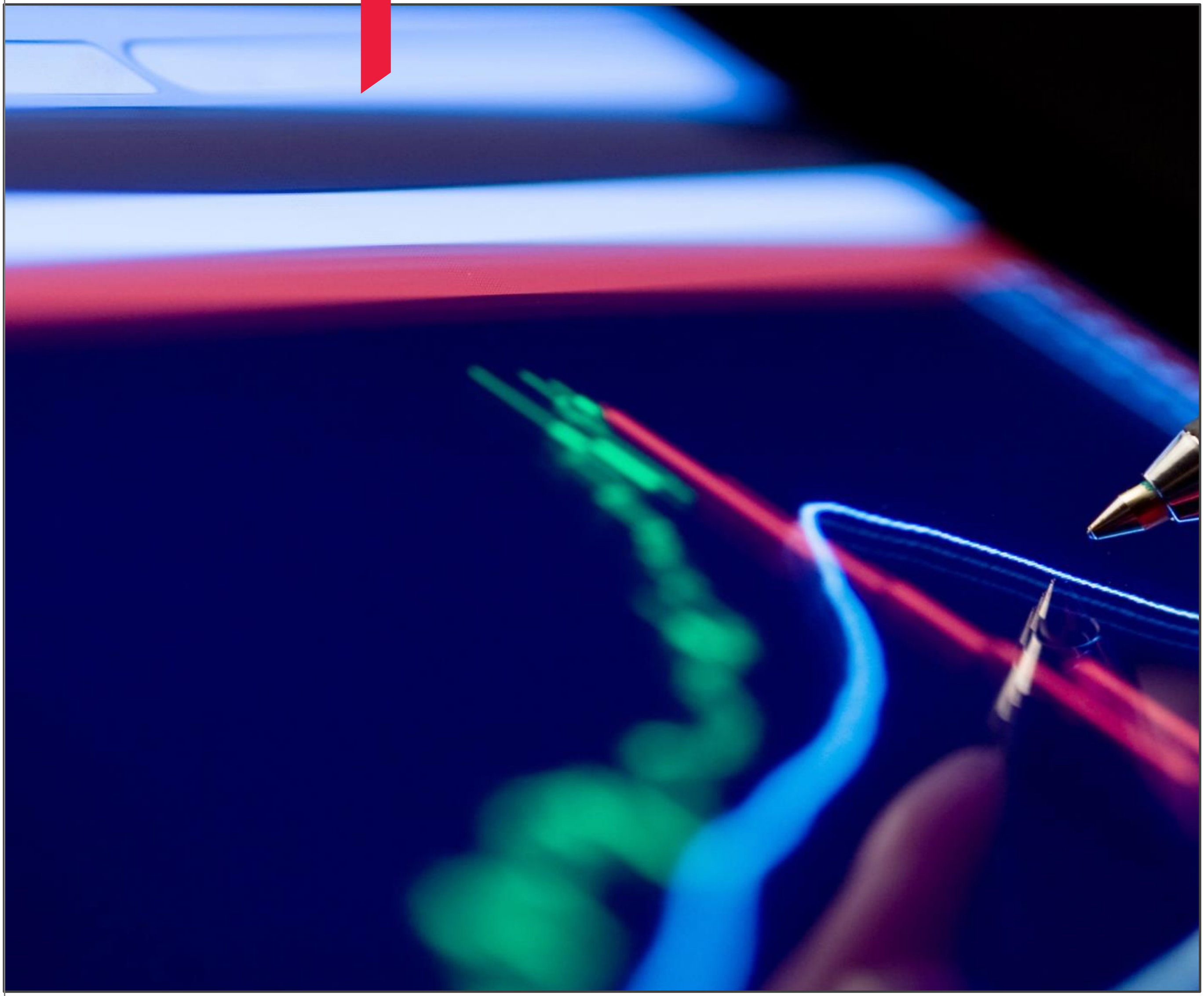

MALDON DISTRICT COUNCIL

INTERNAL AUDIT REPORT

CYBER SECURITY
AUGUST 2023

Design Opinion	● Substantial
Design Effectiveness	● Moderate

IDEAS | PEOPLE | TRUST

CONTENTS

DISTRIBUTION	
Annette Cardy	Resources Specialist Services Manager
Grant Hulley	Lead ICT Specialist (Resources)

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:	Ravi Gadhia - IT Audit Assistant Manager
Dates work performed:	15 February 2023 – 24 May 2023
Draft report issued:	27 June 2023
Final report issued:	15 August 2023

EXECUTIVE SUMMARY

CRR REFERENCE: R11: FAILURE TO PROTECT PERSONAL OR COMMERCIALLY SENSITIVE INFORMATION

Design Opinion	●	Substantial	Design Effectiveness	●	Moderate

Recommendations	0	2	0

SCOPE

BACKGROUND

- Information Technology (IT) systems enable the Council to provide its critical services to its residents and customers and are used to collect, process, and retain ever increasing amounts of confidential information. The vulnerabilities that exist in these IT systems, as well as the infrastructure that supports them, combined with a perceived lack of awareness regarding security issues, have led to attackers targeting public sector organisations and expose the Council to the risk of a cyber security attack.
- Cyber Security is the practice of defending the Council's IT infrastructure, networks, and data from malicious attacks, including computers, servers, mobile devices, and electronic systems. Cyber security attacks can be launched from any internet connection and, as recent examples across the public sector have demonstrated, they can have a significant financial and reputational impact on the Council, impacting its ability to operate and provide critical services to the public.
- The UK Government published a Cyber Security Breaches Survey 2022 report, which provides a detailed overview comprising both quantitative and qualitative research and includes the cost and impact of cyber breaches and attacks on UK businesses, charities, and educational institutions. The survey found that 39% of organisations had identified a cyber-attack over the past 12 months. The most common attack vector remained phishing mails (83%), but one-in-five of these organisations identified a more sophisticated attack such as a denial of service, malware, or ransomware.
- A network security audit was completed in March 2020, which assessed the Council's network security controls and concluded moderate assurance over both their design and their operational effectiveness. The key findings arising from the review included the absence of data and information security training, the absence of appropriate cyber security risk assessments and the absence of internal vulnerability scans to identify and remediate vulnerabilities in relation to how servers and programs are set up.
- In May 2022, the Council suffered a cyber-attack due to a compromised user account. Following the cyber-attack, an action plan was put in place with short-term and long-term actions that have been completed in the subsequent months, including external cyber support from BAE Systems.

AREAS REVIEWED

The following areas were covered as part of this review:

- Assess whether risk assessments in relation to cyber threats are conducted on a regular basis and feed into management decisions on processes deployed
- Determine whether a network diagram is in place and evidences the segregation between trusted and untrusted networks in the infrastructure
- Determine whether information security policies and procedures are regularly reviewed, understood, and adhered to by staff and management
- Assess whether operating systems and application updates and patches are automated and centrally controlled, and whether outstanding updates are known and addressed
- Assess whether firewall rules have been approved and changes or exceptions are securely logged and approved by accountable officers
- Assess whether access to network management console is restricted and whether WPA2 encryption and 802.1X authentication (wired and wireless) has been enabled
- Assess whether antivirus updates are automated and installed on all servers and endpoint devices, and whether outstanding machines are known and addressed
- Assess whether domain administrator access is assigned according to the principle of least privilege, and whether setups are approved, and leavers revoked
- Assess whether external penetration tests and internal vulnerability scans are conducted on a regular basis and whether remediation plans are tracked and overseen by appropriate senior management
- Assess whether incident response plans have been developed and are tested and reviewed for effectiveness on a sufficiently regular basis
- Assess methods of delivering cyber awareness training and the extent of completeness for targeted staff members, and whether outstanding users are escalated to senior management
- Assess whether data recovery and restore plans have been developed and are tested and reviewed for effectiveness on a sufficiently regular basis
- Assess whether communication arrangements have been agreed and approved in the event of a cyber-incident.

AREAS OF STRENGTH

IT Risk Management

- The Council has a Risk Management Policy dated September 2022 which requires all risks and controls to be reviewed on a quarterly basis, in addition to quarterly risk reports (for Corporate Risks Only) being submitted to the Council Leadership Team (CLT) and Performance, Governance and Audit outlining the current risk scores, whether there have been any changes to risk scores and what progress has been made regarding mitigating actions. We reviewed the agenda for the Performance, Governance and Audit Committee dated 15 June 2023 and confirmed that discussions regarding the review of Corporate Risks are taking place.

- The Risk Management Policy states that Service/Operational Risks, Project Risks and Partnership Risks should be subject to regular review and discussed between management and Directors. It is the responsibility of the appropriate managers to ensure that any actions detailed in the business plan to reduce these service risks are taken forward and progress monitored. We were provided with evidence of monthly meetings taking place between the Resources Director, Resources Manager and ICT Manager confirming that monthly meetings are taking place.
- Additionally, the Council also maintains an IT Service/Operational Risk Register. We reviewed the risk register and found this to be comprehensive, setting out a total of 14 risks, each supported by a control owner, existing controls, control strength and date the risk was raised. We noted risks to be around the loss of internet connectivity, loss of power, virtual machine failure, cybersecurity attacks, disk failure and emerging technologies. To support the Council's risk management, we have included an appendix which sets out common IT risks.

IT/Cyber Policies and Procedures

- We were provided with the Council's Information Security Policy and Acceptable Use Policy. We confirmed both policies were reviewed in 1 March 2023 and follow a three year review cycle, with the next review due in March 2026. Both policies are available to all Council staff through the intranet. Our review of the Information Security Policy found this to set out the obligations of all Council staff in terms of protecting IT assets and data, in addition to the roles and responsibilities of staff such as the Senior IT Specialist, Senior Legal Specialist, Directors, Managers and Line Managers, Employees and Members. The Acceptable Use Policy also set out the Council's expectations of staff when using IT assets and the approach taken by the Council in terms of monitoring systems to ensure the Acceptable Use Policy is being adhered to.

Network Security

- The Council has a documented Network Topology Diagram in place. Our review of the network topology found it to clearly define the DMZ (a security network), gateways, servers and switches used in the overall network infrastructure. Overall, the network topology showed a clear segregation between trusted and untrusted networks.
- We were provided with an extract of firewall rules and noted 500 rules in place. All rules related to the Council's Revenue & Benefits system". Our review of the Council's firewall rules, noted that the default firewall rule is to block all traffic unless explicitly specified. Where a user requires a firewall rule to be implemented, a ticket must be raised via the Fresh Service Helpdesk, where tickets are reviewed and approved by the IT Team once the rule has been tested in an isolated testing environment such that it does not affect live systems during testing. We were provided with evidence of a ticket being raised and approved, requesting for a malicious IP address to be blocked to confirm that this process is taking place.
- We were provided with an extract from the Palo Alto Networks firewall which showed a number of encryption techniques being used for both

wired and wireless communications. This includes the 802.1X authentication standard for wired and wireless communications.

- In total, we noted 16 Active Directory accounts with domain administrative privileges, of which two were user accounts, 13 are service accounts (which belong to applications) and one is a Security Group. We were provided with a report from Active Directory which showed that the two user accounts related to two system administrators who have full permissions, while the service accounts were limited to specific functionalities. Passwords for privileged system accounts are managed through the LastPass application, however the Council are planning to use the Bit warden application in the future.

Backups and Patch Management

- We were provided with screenshots confirming that the Council uses Veeam Backup and Replication software to manage the backups of its servers as well as performing server restoration tasks.
- We were also provided with evidence of a full VM (virtual machine) restore being carried out on 24 April 2023 which included five files totalling 120gb. While two errors were noted which were due to a fibre network line and VMWare upgrade, we were provided with further evidence confirming the issues were rectified.
- The Council uses the Endpoint Manager/SCCM application to manage and deploy operating system updates to its IT Estate. We were provided with a report from SCCM which listed a total of 271 devices. We performed analysis to determine how many systems were using builds of Windows still currently supported or not. Out of 271 Windows builds, we noted that all the systems were running on supported operating systems. Although there are 54 systems running on Windows 10 21H1 that are noted as end of service, we noted that they are still receiving extended security updates. The Lead ICT Specialist informed us that the long-term plan for the Council is to migrate all systems to Windows 11 once Windows 10 reaches its end of service lifecycle.

Penetration Testing

- The Council commissioned BAE systems to carry out both external and internal penetration testing which were both carried out in August 2022. The external penetration testing focused on the security of the Council’s Exchange Online servers. In total, 32 recommendations were raised, and we were provided with evidence of an action plan tracking the progress of all the actions.

AREAS OF CONCERN

Business Continuity and Disaster Recovery

- The Council an ICT Business Continuity Plan in place which was last reviewed in September 2019. The IT BCP is significantly out of date due to its last review being in September 2019 and requires a review to ensure it reflects current business practices.
- The Council has in place an ICT Disaster Recovery Plan which was issued in October 2019 and last reviewed in October 2020 and is therefore significantly out of date. While restoration testing has been completed, a test of the DR plan was conducted between 30 April - 02 May 2018 where five findings were raised and hasn’t been subject to a full test since. **Finding 1 (Medium)**

Cyber Security Training

- The Council has a total of 10 IT/Cyber e-learning modules in place for staff to complete. We were provided with a cyber e-learning report for staff regarding the 10 courses. Our review of the report found that 133/261 (51%) staff have not completed all 10 courses. We were provided with a walkthrough of Boxphish which is the system the IT Team use to monitor training compliance. Out of a total of 2,302 courses sent, only 1,707 (74%) courses were completed. **Finding 2 (Medium)**

CONCLUSION

- From our audit work performed, whilst the Council has appropriate controls in place with regards to network and operating system (OS) security, in addition to backup and restore arrangements, further improvement is required in the effectiveness of areas relating to business continuity and disaster recovery and staff. We have therefore provided substantial assurance over the design and moderate assurance over the effectiveness of controls in place.

DETAILED FINDINGS

1	Testing of Business Continuity and Disaster Recovery Plans
TOR Risk:	Critical services, including website hosting, provided by the Council could be disrupted in the event of a cyber-attack, leading to a negative impact on services for residents and customers and the communication of information
Significance	● Medium

FINDING

The Council has in place an ICT Disaster Recovery Plan which was issued in October 2019 and last reviewed in October 2020. Disaster Recovery Plans should be reviewed and tested on an annual basis. However, the latest test of the DR plan was conducted over five years ago, between 30 April - 02 May 2018 where five findings were raised, and it has not been tested since.

The Council also has an ICT Business Continuity Plan in place, but it has not been reviewed since September 2019. Our review of the BCP found it to clearly set out Core Service Functions including telephony, network services and core systems such as Academy, Uniform, Civica and Express as well as a scenario matrix and actions to take in 1 hour, 4 hours, 24 hours, 3 days, and 7 days. The IT BCP also set out a list of activities and who is responsible for carrying out activities and a list of team members and their contact details. However, the IT BCP is out of date due to its last review being in September 2019 and does require a review to ensure it reflects current business practices. Additionally, the IT BCP has not been subject to any testing to confirm whether it is fit for purpose.

However, the above is mitigated to an extent due full restoration testing completed regularly including six-monthly restoration of A Server, A Folder and A file and testing completed on the Council's largest server. PEN testing is also completed annually.

A lack of regular testing around Business Continuity and Disaster Recovery arrangements may lead to inadequate response, ineffective recovery, and unidentified dependencies in the face of potential disruptions to IT.

RECOMMENDATION

a) The Council should review and update the ICT Business Continuity Plan (BCP) on at least an annual basis and ensure it is supported by version control. Additionally, the Council should ensure it also tests its BCP through a desktop exercise, documenting results and actions in order to facilitate continuous improvement.

b) The Council should review and update its ICT Disaster Recovery Plan on an annual basis and ensure it is supported by version control. The Council should also ensure it regularly tests its IT Disaster Recovery plan to ensure it meets Recovery Time Objective (RTO) and Recovery Point Objective (RPO) objectives and we suggest, in addition to the testing noted above, a full test is undertaken in the next 6-12 months

MANAGEMENT RESPONSE

The ICT DR and BCP have now been updated and provided to BDO. These will now be reviewed annually and will be version controlled.

The ICT DR and BPC Planning is tested once a year in three key areas:

1. Host restoration.
2. Internet outage
3. building / disaster

Each of the above are high risk and could mean data loss or no access for staff and members. ICT test from a point of complete loss to a return to full functionality within the RTO and ensure RTO objectives are met. They aim to reduce the RTO each time. The testing is completed with the whole team over a 24-hour period.

A testing schedule has been put in place for July and August of each year. For 2023 testing will be run on 15th Aug 2023.

Responsible Officer:	Grant Hulley - Lead ICT Specialist Resources
Implementation Date:	August 2023

2 Mandatory IT/Cyber Training

TOR Risk:	The Council could incur financial loss and its reputation could be negatively impacted following a successful cyber security attack
Significance	● Medium

FINDING

The Council has a total of 10 IT/Cyber e-learning modules in place for staff to complete which cover: password management, cyber security fundamentals, account takeover, social engineering, identity theft, malware, safe internet usage, physical devices, safe home working and data breaches. We were provided with a walkthrough of Boxphish which is the system that the IT Team use to monitor training compliance. We found that there was only a 74.15% average completion rate across all the courses. A breakdown of completion % per course is noted below:

- Passwords: 100%
- Cyber Security Fundamentals: 88%
- Malware: 85.07%
- Account Takeover: 85.07%
- Social Engineering: 81.9%
- Safe Internet Usage: 80.73%
- Physical Devices: 78.24%
- Data Breaches: 69.26%
- Safe Home Working: 61.51%
- Identify Theft: 71.37%

Absence of appropriate cyber security training may lead to staff being unaware of cyber security best practices which may leave systems vulnerable to attacks from various vectors such as malware, data theft and phishing.

RECOMMENDATION

a) The Council should ensure that all staff members who have not completed IT/Cyber e-learning modules are prompted to do so, with any further instances of non-completion being escalated to line managers for further chasing and further measures taken if non-completion remains.

b) The Council should also produce monthly reports from Boxphish to Senior management detailing IT/Cyber training compliance.

MANAGEMENT RESPONSE

Monthly reports from Boxphish are produced and monitored monthly by IT, the Resources Manager and Director. Staff not completing reports are reminded to do so.

Continued failure to complete courses is then raised with the Resources Manager and SPG Director via reports each month.

Responsible Officer:	Grant Hulley - Lead ICT Specialist Resources
Implementation Date:	September 2023

OBSERVATIONS

MICROSOFT DEFENDER & INTUNE

The Council uses Microsoft Defender across its IT estate for malware and ransomware protection. We were provided with screenshots from Defender which noted that 326 devices have been registered. However, of these, 154 were noted as ‘high exposure’ and 58 have been marked as ‘not onboarded’. We discussed these with the Lead ICT Specialist who informed us that where devices are marked as ‘high exposure’ this relates to user activity as opposed to the security of the device itself, for example – where a user clicks on a malicious link which was blocked by Microsoft Defender. With regards to the 58 devices noted as ‘not onboarded’, we were informed that this discrepancy is a result of the ongoing migration to Microsoft InTune which the Council are currently in the process of completing.

As we were not provided with a device listing from Microsoft Defender (antivirus solution), we were unable to perform any reconciliation between the device listings between Microsoft Endpoint Manager and Microsoft Defender in order to identify any discrepancies.

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:

- Threats to the Council are not adequately identified nor are there procedures in place to prevent vulnerabilities being exploited, resulting in information security becoming compromised
- Critical services, including website hosting, provided by the Council could be disrupted in the event of a cyber-attack, leading to a negative impact on services for residents and customers and the communication of information
- Network authentication and security controls are inadequate and do not effectively prevent unauthorised access to trusted networks, compromising the integrity and security of data and systems
- The Council could incur financial loss and its reputation could be negatively impacted following a successful cyber security attack

SCOPE & APPROACH

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

- Assess whether risk assessments in relation to cyber threats are conducted on a regular basis and feed into management decisions on processes deployed
- Determine whether a network diagram is in place and evidences the segregation between trusted and untrusted networks in the infrastructure
- Determine whether information security policies and procedures are regularly reviewed, understood, and adhered to by staff and management
- Assess whether operating systems and application updates and patches are automated and centrally controlled, and whether outstanding updates are known and addressed
- Assess whether firewall rules have been approved and changes or exceptions are securely logged and approved by accountable officers
- Assess whether access to network management console is restricted and whether WPA2 encryption and 802.1X authentication (wired and wireless) has been enabled
- Assess whether antivirus updates are automated and installed on all servers and endpoint devices, and whether outstanding machines are known and addressed
- Assess whether domain administrator access is assigned according to the principle of least privilege, and whether setups are approved, and leavers revoked
- Assess whether external penetration tests and internal vulnerability scans are conducted on a regular basis and whether remediation plans are tracked and overseen by appropriate senior management
- Assess whether incident response plans have been developed and are tested and reviewed for effectiveness on a sufficiently regular basis
- Assess methods of delivering cyber awareness training and the extent of completeness for targeted staff members, and whether outstanding users are escalated to senior management
- Assess whether data recovery and restore plans have been developed and are tested and reviewed for effectiveness on a sufficiently regular basis

- Assess whether communication arrangements have been agreed and approved in the event of a cyber-incident.

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.

Copyright ©2023 BDO LLP. All rights reserved.