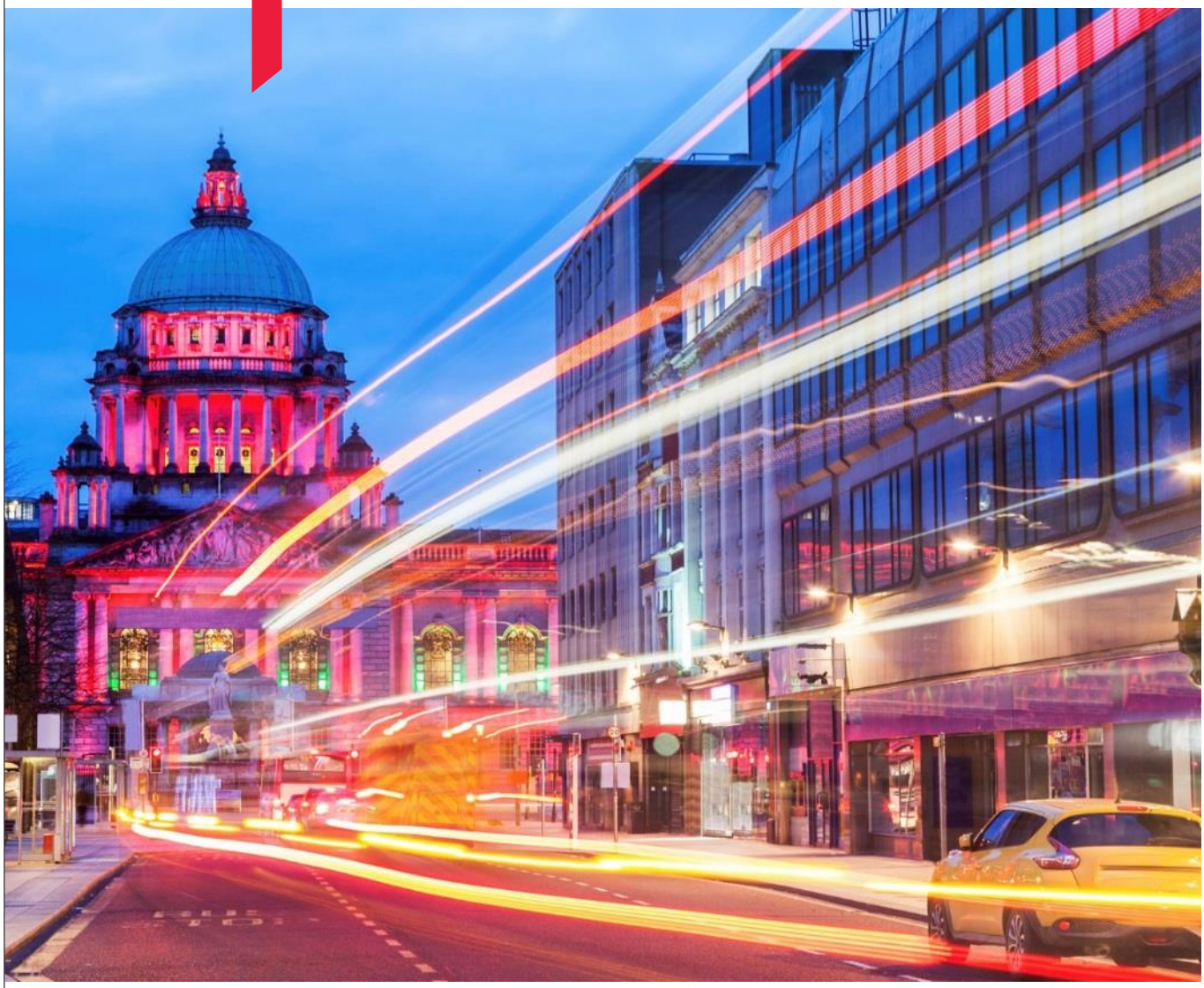

MALDON DISTRICT COUNCIL

INTERNAL AUDIT REPORT - DRAFT

NETWORK SECURITY
MARCH 2020

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Moderate	Moderate

IDEAS | PEOPLE | TRUST

BDO

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

REPORT STATUS LIST	
Auditor	Christopher Culbert – IT Audit Manager
Dates work performed	6 January 2020 – 10 January 2020
Draft report issued	30 January 2020
Final report issued	20 March 2020

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)

Design	Moderate	Generally a sound system of internal control designed to achieve system objectives with some exceptions.
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	3

TOTAL NUMBER OF RECOMMENDATIONS: 7

BACKGROUND:

Information Technology (IT) systems enable the Council to provide their critical services to their customers and are used to collect, process and retain ever increasing amounts of confidential information. The vulnerabilities that exist in these IT systems across the Council, as well as the infrastructure that supports them, combined with a perceived lack of awareness regarding security issues, have led to attackers targeting public organisations and may expose the Council to the risk of a cyber-security attack. Cyber security attacks can be launched from any internet connection and can have a significant financial and reputational impact on the Council.

The Council has undergone a strategic transformation and part of this project was to implement a new network infrastructure, provided by Capita. The new network went live eight months ago. The Council have also changed their patch management protocols, which is now deployed through system centre configuration manager (SCCM). Kaspersky antivirus services and Palo Alto firewalls (program which restricts traffic based on rules set) have also been refreshed and are in place. Other changes from the transformation project include: full redundancy (spare programs in case of failures) for all key network resources, updated password policies, a new password manager tool, and two factor authentication for privileged active directory (AD) accounts (i.e. the user can make key changes to the network).

The next external penetration test is scheduled for March 2020 but a preliminary assessment was undertaken on the external environment following go-live of the new network. Internal vulnerability scanning is also being exercised. Physical network access control mechanisms are also in place which segregate unregistered devices using media access control (MAC) address verification (i.e. only allowed MAC addresses are given access). This represents best practice and leads in comparison to other local authorities which have no network authentication control in place.

GOOD PRACTICE:

Good practice was evidenced in the following areas:

- Network topology (i.e. structure of the network and its components) has been documented following the recent network refresh. The diagram sets out at a high level the key components in place and provides oversight to management to ensure all external routes into the network are protected with Alto Palo firewalls. 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.
- Review of the Aruba network management console showed that WPA2 - Enterprise settings have been enabled (i.e. all wireless traffic between laptops and access points is encrypted)
- Review of the Clear Pass configuration settings showed authentication rules have been enabled for both wireless and wired networks. Hence, only approved devices and user accounts can gain access to the Council's network. The authentication method used complies with the 802.1x standard (i.e. is in line with best practice). Access to the network is not granted unless both the device and user have been approved.
- Review of the password policies set (i.e. password rules) noted passwords must be of at least 15 characters in length, must meet complexity requirements, failed logins limited to 3 attempts, with 1440 min lockout. Hence, are in line with best practice.
- IT health check reports from previous years confirmed external penetration tests have been held. The Head of IT is in the process of commissioning the 2020 external penetration test. A meeting was held on the 16 January to agree in-scope areas. The Public Services Network (PSN) requirements, as set by the Cabinet Office, were used to dictate in-scope areas for both internal and external assessment. The Head of IT has purchasing authority up to £2m for the Council in line with approval from the Director of Resources and so can approve reactive purchases if necessary.

KEY FINDINGS:

We identified the following areas of improvement:

- There has been limited data and information security training provided to all members of staff (**Finding 1 – High)**
- Risk assessments have not been undertaken on a regular basis since December 2017 (**Finding 2 – Medium**)
- There is no internal vulnerability scanning tool in use to identify and remediate vulnerabilities in relation to how servers and programs are setup (**Finding 3 – Medium**)
- At the time of testing there were three live machines with no Kaspersky antivirus installed (**Finding 4 – Medium**)

CONCLUSION:

Overall, we conclude that the control framework in place for the management of identifying, protecting against, detecting, responding and recovering from cyber incidents is adequately designed and operationally effective, but management need to address the areas of risk identified from this review to ensure a robust approach to cyber security is maintained.

DETAILED FINDINGS

RISK: THE COUNCIL IS UNABLE TO RESPOND TO EXPLOITED VULNERABILITIES WHICH LEAD TO NEGATIVE PUBLICITY, LOSS OF REPUTATION, LOSS OF INTELLECTUAL PROPERTY AND DATA BREACHES

Ref	Significance	Finding
1	High	A budget of £20k has been provisionally approved for ICT specialist training. The budget is likely to be committed for the ICT team to attend Aruba and Palo Alto courses, as there is a lack of understanding in usability. The Connect & Learn online portal is being used for all Council eLearning currently. However it was confirmed with finance that subscriptions fees are still being paid for the MetaCompliance tool. GDPR training is compulsory for all staff members. There is no training specific to data and/or information security awareness, which is a critical need for Council staff to minimise the risk of social engineering attacks. There is a reliance on staff having to acknowledge policies on induction.

RECOMMENDATION:

Management should establish a comprehensive induction training program for all new starters, pertaining to information and data security, and track completion with necessary escalations to Heads of Service for non-completion. Management should assess which learning tool is most effective and terminate use and costs for the other.

MANAGEMENT RESPONSE:

Issues and findings were discussed with the Senior ICT Specialist on the 24th January 2020.

IT Password policy and data security will be provided in a package of E learning for staff, this will be a mandatory course to take with an assessment to show correct completion and understanding and a check that IT policies have been read. HR to monitor completion.

Responsible Officer: Annette Cardy

Implementation Date: 30 June 2020

RISK: THE COUNCIL IS UNABLE TO IDENTIFY VULNERABILITIES WHICH LEAD TO FINES, LAWSUITS AND LEGAL FEES RESULTING FROM NONCOMPLIANCE OR LOSS OF CONFIDENTIAL OR CUSTOMER INFORMATION		
Ref	Significance	Finding
2	Medium	In 2017 the previous Head of ICT performed a comprehensive assessment of all cyber risks in line with the National Cyber Security Centre (20 Critical Controls) guidance. A cyber risk register was developed which identified and assessed the residual risk of all cyber risk at the time. Further to this, cyber training was developed for staff members to aide in mitigating some of the cyber risks relevant to social engineering and weak security controls. There has been no cyber risk assessment conducted since December 2017. Continual review and assessment of risks is needed to ensure mitigating actions remain adequate.

RECOMMENDATION:

Cyber risk assessments should be undertaken on a regular basis in order to update mitigating actions in the cyber risk register.

MANAGEMENT RESPONSE:

Issues and findings were discussed with the Senior ICT Specialist on the 24th January 2020.

An ITHC is scheduled to run in March which will include a cyber risk assessment on the DR plan, using these results the risk register will be updated and then actioned. Actions will be completed, and Re-test will be completed every 6 months.

Responsible Officer: Grant Hulley

Implementation Date: 31 May 2020

RISK: THE COUNCIL IS UNABLE TO DETECT EXPLOITED VULNERABILITIES WHICH LEAD TO NEGATIVE PUBLICITY, LOSS OF REPUTATION, LOSS OF INTELLECTUAL PROPERTY AND DATA BREACHES		
Ref	Significance	Finding
3	Medium	The Council has never used any internal vulnerability scanning tools. Reliance has been solely placed on the annual penetration test of internal areas. However, this is not conducted sufficiently regularly and will not identify all potential vulnerabilities. Management need to perform a cost assessment of implementing an internal vulnerability scanning tool against the benefits of identifying vulnerabilities in inappropriate user access, configuration vulnerabilities, and unnecessary open ports on critical hosts in the network. Considerations of costs should include resource needs for remediating on a monthly basis.

RECOMMENDATION:

Management should perform a cost: benefit assessment for implementing an internal vulnerability scanning tool.

MANAGEMENT RESPONSE:

Issues and findings were discussed with the Senior ICT Specialist on the 24th January 2020.

MDC have now installed the OpenVAS scanning tool

Responsible Officer: Grant Hulley

Implementation Date: Completed

RISK: THE COUNCIL IS UNABLE TO DETECT EXPLOITED VULNERABILITIES WHICH LEAD TO NEGATIVE PUBLICITY, LOSS OF REPUTATION, LOSS OF INTELLECTUAL PROPERTY AND DATA BREACHES		
Ref	Significance	Finding
4	Medium	Kaspersky agents are installed with all new devices as part of standardised build procedure. Review of scheduled tasks on the Kaspersky program confirmed automatic updates are run on all machines. Review of Kaspersky Security Centre showed automatic updates every one hour had been enabled. Review of the dashboard showed several definition update failures and non-responsive clients. It is known that there are redundant devices with clients installed which need to be removed. Review of standardised machine build showed installation of Kaspersky as the final process run. Hence, all new devices have Kaspersky installed at build stage. Reconciliation of Kaspersky clients to machines registered to domain in AD identified a total of 15 machines which are registered to the domain but have no Kaspersky client installed on them. Further review confirmed only three machines are not on client listing, but eight are assigned to the wrong management group (i.e. wrong A/V policies applied). Four are public machines which are segregated from the network. We also identified three machines with Kaspersky clients installed on them but are no longer registered to the domain (i.e. redundant machines).

RECOMMENDATION:

Management should install antivirus clients on outstanding machines in use and registered to the network domain.

MANAGEMENT RESPONSE:

Issues and findings were discussed with the Senior ICT Specialist on the 24th January 2020.

All Client machines now have the full AV installed.

Responsible Officer: Grant Hulley

Implementation Date: Completed

RISK: THE COUNCIL IS UNABLE TO PROTECT AGAINST THREATS WHICH LEAD TO NEGATIVE PUBLICITY RESULTING IN LOSS OF REPUTATION AND LOSS OF INTELLECTUAL PROPERTY OR TRADE SECRETS		
Ref	Significance	Finding
5	Low	Review of the utility report administrators showed a total of four users and one service account. Four users were confirmed to be global administrators in the ICT team. The service account was for redundancy firewall communication. To date the ICT team have used a manual worksheet to document changes and approval to firewall rules, but this has not been consistently used and does not enforce approval. A move to the help desk (FreshDesk) would provide a complete trail and also enforce approval from an ICT Specialist.

RECOMMENDATION:

Management should use the FreshDesk workflow system to document and approval changes to firewall rules.

MANAGEMENT RESPONSE:

Issues and findings were discussed with the Senior ICT Specialist on the 24th January 2020.

IT now utilising FreshService as a central point to monitor all staff use including firewall. Completed.

Responsible Officer: Grant Hulley

Implementation Date: Completed

RISK: THE COUNCIL IS UNABLE TO PROTECT AGAINST THREATS WHICH LEAD TO NEGATIVE PUBLICITY RESULTING IN LOSS OF REPUTATION AND LOSS OF INTELLECTUAL PROPERTY OR TRADE SECRETS		
Ref	Significance	Finding
6	Low	Server 2008 is not running on any live machines. SCCM clients run on 214 in Win10 group (1909 version of Windows) - this ensures SCCM deploys to them. SCCM polls for updates on a weekly basis - restricted to critical and high releases. There are no test machines or servers in place to allow for errors due to budgetary constraints. Deployment schedules run on a weekly basis. Review of deployment logs showed: only 14 in progress (error code 0x000000), only 4 in error (review showed two were redundant so to be removed, two others can be checked), total of 43 devices listed (however 19 of which passed check and were active). As deployments are run weekly there is no need for intra-monthly exception deployment schedules.

RECOMMENDATION:

Management should address the OS update deployment failures in a timely manner going forwards.

MANAGEMENT RESPONSE:

Issues and findings were discussed with the Senior ICT Specialist on the 24th January 2020.

This is checked within a 24 hour period of all updates and is monitored

Responsible Officer: Grant Hulley

Implementation Date: Completed

RISK: THE COUNCIL IS UNABLE TO PROTECT AGAINST THREATS WHICH LEAD TO NEGATIVE PUBLICITY RESULTING IN LOSS OF REPUTATION AND LOSS OF INTELLECTUAL PROPERTY OR TRADE SECRETS		
Ref	Significance	Finding
7	Low	Policies were developed and uploaded onto the intranet in 2018 for Access Control, Email and Communications, Acceptable Usage, and Information Security. The Information Security policy needs updating in relation to staff changes but holds adequate responsibilities for key officers in the organisation. The Information Security Incident Reporting and Management Policy has been comprehensively written and captures the key requirements as set out in ISO 27001. However, there is no protocol in place to keep these policies under regular review going forwards. Policies need to be regularly reviewed and disseminated to staff to ensure they relate to current practices and maintain awareness.

RECOMMENDATION:

Information and data security policies should be regularly reviewed and approved by appropriate sub-committee members going forwards.

MANAGEMENT RESPONSE:

Issues and findings were discussed with the Senior ICT Specialist on the 24th January 2020.

Password and other IT policies will be reviewed and approved at R&S Committee in June 2020 with a programme of review.

Responsible Officer: Grant Hulley

Implementation Date: End June

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
Craig Smith	Specialist - ICT Applications
James Wright	ICT Specialist - Resources Directorate

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:

This audit appraised the design and operational effectiveness of the Council's procedures for identifying and protecting its information assets and for managing its cyber security risks on an ongoing basis.
Our work was designed to provide an assessment of the information asset and cyber security arrangements that are in place, but cannot provide absolute assurance that the Council would withstand an attack of its systems.

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 Council is unable to identify vulnerabilities which lead to fines, lawsuits and legal fees resulting from noncompliance or loss of confidential or customer information
- The Council is unable to protect against threats which lead to negative publicity resulting in loss of reputation and loss of intellectual property or trade secrets
- The Council is unable to detect exploited vulnerabilities which lead to negative publicity, loss of reputation, loss of intellectual property and data breaches
- The Council is unable to respond to exploited vulnerabilities which lead to negative publicity, loss of reputation, loss of intellectual property and data breaches
- The Council is unable to recover from exploited vulnerabilities which lead to forensic investigation costs, technology improvement costs, and loss of time and productivity

SCOPE OF REVIEW:

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

- Security threats to the Council have been identified and assessed and action has been taken to prevent vulnerabilities from being exploited
- Members of staff are provided with adequate training and awareness
- Appropriate IT network security controls have been deployed and are operational
- The efficacy of the IT network security controls is reviewed on a routine basis
- There are defined procedures in place for responding to and recovering from an incident

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