Audit Agenda

Wednesday 19 July 2017 at 7.30 pm

Conference Room 2 - The Forum

The Councillors listed below are requested to attend the above meeting, on the day and at the time and place stated, to consider the business set out in this agenda.

Membership

Councillor Brown
Councillor Douris
Councillor McLean
Councillor Taylor (Chair)
Councillor Tindall
Councillor W Wyatt-Lowe

Substitute Members:
Councillors G Adshead, Anderson, England, Link and Ransley

For further information, please contact Jim Doyle

AGENDA

(a) Cyber Essentials - DBC Final Report (Pages 2 - 14)

MAZARS

Dacorum Borough Council

Final Internal Audit Report

Cyber Essentials

July 2017

This report has been prepared on the basis of the limitations set out on page 10.

CONFIDENTIAL

Distribution List:

Ben Trueman – Group Manager, Technology and Digital Transformation

David Skinner – Assistant Director, Finance & Resources

James Deane – Corporate Director (Finance and Operations) (Final Report only)

Sally Marshall – Chief Executive (Final Report only)

Key Dates:

Date of fieldwork:	May/June 2017
Date of draft report:	June 2017
Receipt of responses:	July 2017
Date of final report:	July2017

Contents

1. Executive Summary

1.1. Background

Her Majesty's Government (HMG) introduced the "Cyber Essentials" Scheme in April 2014 to provide clarity to organisations on what good cyber security practice is and the steps they need to follow to help manage cyber risks, i.e. impact on confidentiality, integrity and availability of system data that is stored and supported by ICT Services.

Given the nature of the threat, Government believes that action should begin with a core set of baseline controls which all organisations should apply and demonstrate in order to confidently conduct business securely.

Therefore, Dacorum Borough Council (DBC) were looking for assurance that their key information security controls are in line with those proposed by the UK Government in the 'Cyber Essentials' programme.

1.2. Audit Objective and Scope

The overall objective of the audit was to evaluate and test the controls over the following areas, based on the UK Government's Cyber Essentials framework:

- Boundary Firewalls and Internet Gateways
- Secure Configuration
- Access Control
- Malware Protection
- Patch Management

Further detail on the scope of the audit is provided in Section 2 of the report.

1.3. Summary Assessment

Our audit of DBC's internal controls in operation against best practice, as set out within the Governments Cyber Essentials Scheme found that, there is a sound system of internal control designed to achieve the system objectives. However, there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Our assessment in terms of the design of, and compliance with, the system of internal control covered is set out below:

Evaluation Assessment	Testing Assessment
Full	Substantial

Management should be aware that our internal audit work was performed according to UK Public Sector Internal Audit Standards (PSIAS) which are different from audits performed in accordance with International Standards on Auditing (UK and Ireland) issued by the Auditing Practices Board. Similarly, the assurance gradings provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

The classifications of our audit assessments and priority ratings definitions for our recommendations are set out in more detail in Appendix A, whilst further analysis of the control environment is shown in Section 3.

1.4. Key Findings

One Priority 2 and three priority 3 recommendations were raised where we believe there is scope for improvement within control environment. These are set out below:

- Formally document the current Back Up process and carry out periodic restore tests (Priority 2)
- Update the Disaster Recovery Policy and supporting documentation (Priority 3)
- Put in place a clear schedule for updating third party software (Priority 3)

- Formally document the Patch Management process to ensure consistent approach (Priority 3)

Full details of the audit findings and recommendations are shown in Section 4 of the report.

1.5. Management Response

We received the management responses in a timely manner and these have been included in the main body of report.

1.6. Acknowledgement

We would like to take this opportunity to thank all staff involved for their time and co-operation during the course of this visit.

2. Scope of Assignment

2.1. Objective

The overall objective of this audit was to provide assurance on the design and operation of the controls applied in respect of the UK Governments Cyber Essentials Scheme.

2.2. Approach and Methodology

The audit approach was developed by an assessment of risks and management controls operating within each area of the scope and the following procedures were adopted to enable us to recommend control improvements:

- Hold discussions with key members of staff to ascertain the operational controls;
- Identification of the role and objective of each area of scope;
- Identification of risks relating to the auditable area and the controls in place that enable the control objectives to be achieved;
- Evaluation and testing of controls within the system;
- Discussion of our findings with management and further development of our recommendations; and
- Preparation and agreement of a draft report with the process owner.

2.3. Areas Covered

The audit was carried out to evaluate and test controls over the following areas:

- **Boundary Firewalls and Internet Gateways**
  Sufficient protection from external attack exists at all points on the network perimeter which are accessible by the wider Internet.
- **Secure Configuration**
  All desktop, mobile, perimeter, and infrastructure devices are configured in a secure manner.
- **Access Control**
  Access is restricted per user to an extent by which they are only able to view, edit, or otherwise use information or assets they are permitted to as part of their role.
- **Malware Protection**
  All devices are sufficiently protected from malicious software. This includes logical mechanisms such as anti-virus software, as well as training and awareness to aid in preventing users from emplacing malicious software on the organisation's internal network.
- **Patch Management**
  All desktops, servers, and mobile devices are patched in a timely manner as they are released.

3. Assessment of Control Environment

The following table sets out in summary the control objectives we have covered as part of this audit, our assessment of risk based on the adequacy of controls in place, the effectiveness of the controls tested and any resultant recommendations.

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.

Control Objectives Assessed	Design of Controls	Operation of Controls	Recommendations Raised
Boundary Firewalls & Internet Gateways			
Secure Configuration			**Recommendation 1 (P2), 2 (P3), 3 (P3)**
User Access Controls			
Malware			
Patch Management			**Recommendation 4 (P3)**

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.

4. Observations and Recommendations

Recommendation 1: Formal Back Up Policy (Priority 2)

Recommendation

Management should ensure that a Backup Policy is developed and implemented. This should incorporate in addition to other elements:

- Backup regime;
- Backup data retention; and
- Backup restorability tests.

Observation

A backup policy gives guidelines on how backup is made, which backup regime to be used, which critical systems to prioritise, how long data backup should be retained and a schedule of data backup integrity tests. This ensures that data can be restored from backup as when needed.

During the audit, we established that a formally documented backup policy was not in place. Data backup retention was not defined or formally documented. Additionally, audit could not find evidence of any scheduled restorability tests performed on data that is held as backup.

Without a documented back up policy and schedule of restore testing in place, there is a risk that staff may not be fully aware of the current working arrangements or if the data can be fully restored in the event of failure leading to a potential loss of data.

Responsibility

Group Manager – Technology & Digital Transformation

Management response / deadline

Although there is no suggestion in the report that backups were being undertaken any less frequently or effectively than they should have been, we recognise the benefits of codifying this existing good practice and will develop appropriate documentation.

We will have a fully prepared backup policy documented and in use by the end of August 2017. This will include practical guidelines, prioritisation and retention timelines (developed in collaboration with the Council's Information Security Officer).

We will undertake restorability tests on a bi-monthly basis, with the first one scheduled for end of August 2017.

Recommendation 2: Update Disaster Recovery Policy (Priority 3)

Recommendation

The Disaster Recovery policy and supporting documentation should be updated to ensure it continues to reflect the current working practices of the organisation following the decommissioning process of the severs running windows 2003.

Observation

An up to date Disaster Recovery Policy will give an organisation a clear and precise process to follow in the occurrence of a significant event to ensure it can recover as efficiently and effectively as possible.

From review of the action plan produced following the recent ITHC, it has been established that a number of servers running windows 2003 are in the process of being decommissioned and as a result the Disaster Recovery policy and supporting documentation will not continue to accurately reflect the working practices of the organisation.

Without an up to date Disaster Recovery Policy and supporting documentation there is a risk that in the event of any significant occurrence the organisation may not be able to recover the services in an effective and timely fashion.

Responsibility

Group Manager – Technology & Digital Transformation

Management response / deadline

At the point of the audit a number of Windows 2003 servers were in the process of being taken out of service. As the decommissioning process was not complete references remained within the Recovery Plan.

Since these servers have been fully decommissioned, they have been removed from the High Level Recovery Plan, which accurately reflects the current server estate. We will continue to update this document to reflect both newly commissioned and decommissioned machines.

Recommendation 3: Software Monitoring (Priority 3)

Recommendation While the Council has a robust system for applying critical operating system security updates, it should ensure it puts in place a clear schedule for updating third party software.
Observation Having a formal review schedule ensures the software in use remains up to date and in line with current support arrangements. From an examination of the PSN compliance review and subsequent action plan, it has been established that there were instances where out of date software was in use and updates were available but had not been implemented. From a review of the action plan produced and discussion with the ICT department it is evident that these specific incidents have been addressed and software updated or removed where applicable. Without a formal schedule of review in place, there is a risk of running out of date software which could result in a potential breach of support arrangements, the Council not obtaining support should there be an issue with the software or not obtaining the benefits of the updated software.
Responsibility **Group Manager – Technology & Digital Transformation**
Management response / deadline As the report indicates, this finding is based on information from the PSN mandated IT Health Check of August 2016. All related patches have been deployed (and had been well in advance of this audit). Critical and security Operating System updates are automatically deployed on a fixed schedule. This is fortnightly for servers and immediately on release for client devices. With any fixed schedule, there will be always be moments in time when patches have been released by suppliers but not yet deployed. 3rd party patches are always more technically challenging. However, the Council is developing a schedule for the automatic deployment of these. This will be complete by the end of August 2017.

Recommendation 4: Patch Management Policy (Priority 3)

Recommendation

A formally documented patch management policy and procedure should be developed which demonstrates that a rolling schedule of phased updates is in place to help ensure that systems are maintained and kept up to date with the right patches to help protect the network from known vulnerabilities.

The organisation should also consider producing detailed patch and vulnerability management compliance monitoring reports and agree high level Key Performance Indicators to monitor the effective delivery of security patch management activities.

Observation

Up to date policies and procedures ensure that patches are applied in a reasonable timescale and systems are maintained and kept up to date with the right patches to help protect the network from known vulnerabilities.

Whilst scheduled patching does take place by means of automatic deployment for both the Windows services and 3rd party applications, there is no formal Patch Management Policy in place which clearly defines roles and responsibilities, the patching schedule, monitoring and reporting arrangements or escalation procedures in the event of failure.

At the time of the review, audit were provided with a copy of the latest MBSA (Microsoft Security Baseline Analyser) report (April 2017) which highlighted a number of outstanding critical security patches. However, from conversations with ICT it was indicated that these reports are run regularly and areas for action are addressed accordingly.

Monitoring reports or key performance indicators are not currently in place to help ensure that that patches are being implemented as intended.

Unless automated patch management activity reporting is established and appropriate key performance indicators (KPIs) are agreed to monitor the effective achievement of security patch management, there is an increased risk that the network will be open to high risk vulnerabilities.

Missing application security updates increases the risk that cyber attackers may be able to access and exploit known application system vulnerabilities.

Responsibility

Group Manager – Technology & Digital Transformation

Management response / deadline

The report indicates that the patch management policy is in place and being actioned appropriately.

Also as noted above, Critical and security Operating System updates are automatically deployed on a fixed schedule. This is fortnightly for servers and immediately on release for client devices. With any fixed schedule, there will be always be moments in time when patches have been released by suppliers but not yet deployed.

However, to provide more visible assurance on this, we will investigate the introduction of KPIs and associated reporting with a view to introducing new indicators in 2018/19, subject to agreement with the Council's Performance team.

Appendix A - Reporting Definitions

Audit assessment

In order to provide management with an assessment of the adequacy and effectiveness of their systems of internal control, the following definitions are used:

Level	Symbol	Evaluation Assessment	Testing Assessment
Full		There is a sound system of internal control designed to achieve the system objectives.	The controls are being consistently applied.
Substantial		Whilst there is a basically sound system of internal control design, there are weaknesses in design which may place some of the system objectives at risk.	There is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
Limited		Weaknesses in the system of internal control design are such as to put the system objectives at risk.	The level of non-compliance puts the system objectives at risk.
Nil		Control is generally weak leaving the system open to significant error or abuse.	Significant non-compliance with basic controls leaves the system open to error or abuse.

The assessment gradings provided here are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board and as such the grading of 'Full' does not imply that there are no risks to the stated control objectives.

Grading of recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows:

Level	Definition
Priority 1	Recommendations which are fundamental to the system and upon which the organisation should take immediate action.
Priority 2	Recommendations which, although not fundamental to the system, provide scope for improvements to be made.
Priority 3	Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed.
System Improvement Opportunity	Issues concerning potential opportunities for management to improve the operational efficiency and/or effectiveness of the system.

Appendix B - Staff Interviewed

The following personnel were consulted:

Audit sponsor:	David Skinner – Assistant Director, Finance & Resources
Audit Contacts:	Ben Trueman – Group Manager, Technology and Digital Transformation
Auditee Contacts:	Gary Olser – ICT Operations Team Lead
	Ian Swinton – ICT Networks
	Robbie File – Business Systems Developer
	Alan Parry – Orchard Application Systems Lead
	Stuart Potton - Revenues & Benefits Support Team Leader

We would like to thank the staff involved for their co-operation during the audit.

Statement of Responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by us should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Our procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our work and to ensure the authenticity of such material. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

Mazars Public Sector Internal Audit Limited

London

July 2017

In this document references to Mazars are references to Mazars Public Sector Internal Audit Limited.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom. Registered in England and Wales No 4585162.

Mazars Public Sector Internal Audit Limited is a subsidiary of Mazars LLP. Mazars LLP is the UK firm of Mazars, an international advisory and accountancy group. Mazars LLP is registered by the Institute of Chartered Accountants in England and Wales to carry out company audit work.