APPENDIX 3 – Executive Summaries finalised since last update to Accounts, Audit & Risk Committee June 2021

CDC Cyber Security Follow Up 2021/22

Opinion: Amber	
Total: 9	Priority 1 = 0 Priority 2 = 9
Current Status:	
Implemented	4
Due not yet actioned	1
Partially complete	1
Not yet Due	3

Introduction

Cyber threats are not new, but the focus on cyber security remains important because of the number of high-profile security incidents and data breaches. Hackers, cyber-criminals and nation states have a range of motives for stealing, disrupting or destroying information and the IT systems that rely upon them. The consequences of a data breach include operational disruption, regulatory fines and reputational damage.

A review of Cyber Security was undertaken as part of the internal audit plan for 2020/21. The audit resulted in an “amber” conclusion and 15 management actions were agreed to address the areas of risk identified. Three supplementary issues were also raised.

Scope of work

The scope of this audit was limited to carrying out a follow-up of the agreed management actions to confirm their current status. Testing was undertaken to verify actions that are reported as being fully implemented.

Overall Conclusion

Our overall conclusion on the system of internal control relating to Cyber Security remains as Amber. Some progress has been made with agreed management actions but a number remain outstanding as detailed below.

Of the 15 ‘priority 2’ management actions arising from our Cyber Security review in 2020/21, 5 have been fully implemented, 3 partly implemented and one superseded. However, there are 6 actions which have not been completed and thus remain outstanding. These include the following:

- Ensuring corporate IT security policies cover key areas of cyber security;
- Developing the Cyber Threat document into a full Cyber Incident Response Plan;
- Commissioning a phishing test. The Cyber Security Officer has confirmed that this will form part of the Cyber Security Awareness Project which has recently been approved;
- Reviewing the users outside IT Services who have administrator access on certain servers;
- Displaying a network logon message to make all users aware of corporate IT security policies; and
- Reviewing the status of Windows Defender malware protection on all end points – this was addressed during the audit.

CDC IT Remote Working 2021/22

Overall conclusion on the system of internal control being maintained	**A**

RISK AREAS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
Corporate Policies	**A**	**0**	**2**
Remote Access Solution	**G**	**0**	**1**
Hardware Assets	**A**	**0**	**4**
Device Security	**A**	**1**	**2**
Collaboration Tools	**G**	**0**	**1**
		1	**10**

Opinion: Amber	
Total: 11	Priority 1 = 1 Priority 2 = 10
Current Status:	
Implemented	5
Due not yet actioned	1
Partially complete	0
Not yet Due	5

One of the biggest challenges posed by the Covid-19 pandemic was the need to rapidly move to remote/home working. Whilst the ability to work remotely was available before the pandemic, it had to be scaled up quickly to support the majority of staff working at home. A hybrid model of remote working is likely to remain for certain staff and hence it is important that the council has controls in place to manage the risk associated with this, especially in regard to data security.

There are corporate policies on remote working, namely the Home Working Policy and the IT Mobile Device Policy. The former is dated April 2013 and needs to be updated to include current standards and requirements for home working and neither policy makes any reference to remote access or the security and storage of paper records. The two policies also still refer to the Data Protection Act 1998, which was superseded in 2018.

Remote access to the corporate network, Microsoft Cloud and other cloud-based applications is subject to multi-factor authentication in accordance with good practice. This requires users to enter their network username and password, together with an additional level of authentication using either the Microsoft Authenticator App or a text message to a mobile phone. Microsoft conditional access is used to block remote access from certain high-risk countries. There are a small number of users who use Citrix for remote access and we found they are also subject to multi-factor authentication, although we noted that Citrix still supports an old security protocol with known security vulnerabilities which presents a cyber risk.

There is an inventory of computers and mobile devices. We have identified weaknesses in its management which presents a risk that individual assets cannot be identified or accounted for. The computer inventory is held within the IT service management tool but an error with a scheduled overnight task, identified during the audit, means the data has not been updated since March 2020. The staff leaver's process does not ensure that all IT equipment is returned and there are no records of the computer equipment held in storage and hence any missing or stolen items may not be quickly identified. Access to the computer inventory is also not adequately restricted to prevent unauthorised changes being made to data.

All computer laptops are encrypted and there is a security policy applied to mobile devices which requires them to be password protected and also encrypted. There are currently no tools to remotely wipe a lost or stolen mobile device, restrict the downloading of applications or access to certain services. This requires a mobile device management system which should be investigated. Users are not prevented from copying data onto untrusted USB storage devices and this poses a significant risk in regard to data protection compliance and cyber security. Some users are allowed to use personal devices to access corporate systems e.g. email, but they are not made aware of the "Bring Your Own Device" policy before their device is authorised for use, to ensure they are aware of their responsibilities.

There is a legacy collaboration tool called 8x8 but the main tool is Microsoft Teams, which comes with user guidance documents and videos that available on the agile working pages of the Intranet. A review of the meetings policy on Teams identified a risk as it is not locked down to prevent unauthorised users from accessing online meetings.

CDC PCI DSS Compliance 2021/22

Overall conclusion on the system of internal control being maintained	**R**

RISK AREAS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
Corporate Structure	**R**	**1**	**0**
PCI Scope	**R**	**0**	**2**
PCI Security Controls	**R**	**2**	**3**
Network Security Scans	**A**	**0**	**1**
		3	**6**

Opinion: Red	
Total: 9	Priority 1 = 3 Priority 2 = 6
Current Status:	
Implemented	2
Due not yet actioned	0
Partially complete	0
Not yet Due	7

All organisations that store, process or transmit cardholder data must comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS defines technical and operational security requirements set by the PCI Security Standards Council to protect all cardholder data.

Our sample testing has not identified any service areas where the council hold card payment details. However, card payments are taken by a number of services, mainly via the Capita Pay360 payment system, and thus there is an obligation on the council to ensure such payments are taken securely in accordance with PCI DSS. We have found there is currently a weak control framework over PCI compliance, resulting in a number of key risks, including potential fines, penalties and reputational damage as a result of cardholder data being compromised. The key issues identified are:

- The organisation’s overall approach to meeting PCI requirements is not set out in a formal policy;
- PCI roles and responsibilities are not defined and thus there is no ownership of compliance activities;
- All merchant activities have not been identified i.e. areas of the council where card payments are taken, including how they are taken e.g. on-line, telephone, face-to-face;
- The PCI environment is not scoped in terms of people, processes and technology to ensure a complete and accurate compliance assessment can be undertaken;
- A Self-Assessment Questionnaire (SAQ) is not completed annually, as required by PCI DSS, resulting in any gaps in control not being identified and remediated;
- The PCI compliance status of third-party service providers is not verified to confirm that their processing complies with PCI requirements and there are also no documented procedures for managing these third-parties;
- There is no documented procedure for dealing with telephone calls in the contact centre that do not stop recording when card payments are taken and we have found that such recordings are not always deleted;
- Staff who take card payments have not been provided with any training or awareness on PCI requirements and thus may not be aware of their responsibilities for securing card details; and
- Security scans are not currently performed as it has not been confirmed if they are required. The need for security scans is dependent on merchant activities and the relevant SAQ (see above).

Our testing has confirmed that all users have unique accounts on the Capita Pay360 payment application and the password policy complies with PCI requirements.

PCI DSS Internal Audit Report 2021/22 – Management Response

Finance is grateful to the Internal Audit Team for bringing the recommended management actions identified in CDC’s control framework over PCI compliance to our attention. This gives us the opportunity to make improvements to our processes. All of the audit findings and suggested management actions have been accepted.

The Council is working with its partners that already have significant experience of PCI compliance. They are providing significant support to help the Council to swiftly develop and implement the necessary policies and procedures and to guide us through the remaining actions the Council needs to take.

The Council is prioritising the implementation of these actions and has already developed a Credit/Debit Card Income Collection Policy which was approved on 28 July 2021; this is the overarching policy for PCI. A number of policies that will sit below this are now being developed and finalised. Additionally, new chip and pin machines have been installed where necessary.