Area of Review	**IT Controls**
Level of Assurance	Limited Limited assurance is given where controls in place are not always applied and objectives may not be achieved, meaning the Council is exposed to the risk of financial loss, fraud or the loss of reputation.

Objectives of Review

1. That network access is effectively managed
2. That assets are securely held
3. That effective data management arrangements are in place
4. That appropriate continuity arrangements are in place

Key Findings

- The Active Directory (AD) is not well managed. This means there is a risk of unauthorised access to the network from either a former employee of Capita or the Council. It only takes one disgruntled employee to cause significant issues. There are 146 Capita user Accounts on the AD, it is highly likely that some will no longer be working on our contract.
- There is not a consistent approach to the management of leavers, in particular with Capita employees. This has resulted in user accounts remaining live on Hart's network for longer than required, which again increases the risk of unauthorised access.
- The Council is using servers that are running on Windows 2003. Which is software that is no longer supported by Microsoft. This means that security updates are not downloaded to these servers. It is noted that these servers are firewalled from the rest of the network, and that in some cases decommissioning is planned, however they still remain at risk from cyber threats.
- Virus protection is up to date for all other servers and desktops. Although Laptops are not always updated in a timely manner.
- The Council does not have an up to date Public Sector Network Certificate. This means there is a risk that the councils would not be able to send or receive data over the internet with other public sector bodies. The lack of an up to date assessment also has an impact on other security tests, such as penetration testing and password cracking which are effective tools for identifying security vulnerabilities. Whilst the above risks are valid, it is noted that the Cabinet Office have agreed that a new certificate is not required until the transition to the new Capita IT Platform is complete.
- There is reasonable assurance that password protocols comply with good practice.
- IT Security Policies are in place, however they were last reviewed in April 2016.
- Cyber Security Training was provided to all employees during 2018/19. Training was also made available to members.
- There is not an up to date inventory of IT Assets, without such an inventory there is a risk that the Council would not be able to confirm what devices have been allocated to

employees. This is particularly important for the more portable devices such as Laptops, IPads and Mobile Phones.

- Progress has been made on data management since our last review 12 months ago, further improvements are planned. Risks around data retention and accuracy of data held still remain. Further work is needed to ensure we do not migrate out of date and inaccurate data to Sharepoint.
- There is reasonable assurance that backup arrangements are robust.
- The IT Business Continuity Plan is unlikely to be workable in its current form. The plan is based around our service being provided in Southampton, which may not be the case under the 5 Councils contract.

MANAGEMENT ACTION PLAN

	Recommendation	Responsible Officer	Risk Level	Officer Response	Target Date
1.	Carry out a full review of the Active Directory.	IT Client Officer	High	Hart staff are effectively managed through the O365 portal. Capita staff are the biggest risk. The AD will be reviewed and any Capita employees identified on the report that are no longer working on the 5 Council's Contract will be deleted.	March 2019
2.	Establish an effective process for managing the Active Directory that ensures full control of the AD is not soley with Capita.	IT Client Officer	High	One option for the effective management is for the IT Client/Hart to authorise the creation of any new Capita or Hart User Account. This will be discussed with Capita.	March 2019
3.	Ensure that the 45 day rule for disabling inactive accounts is re-	IT Client Officer	High	Raised with the 5 Councils Client Officer to ensure that	March 2019

	established, as is the 90 day rule for deleting such accounts.			the existing automatic process is followed for all staff.	
4.	Review Capita employees that currently have System and Domain Admin rights to ensure they are still valid.	IT Client Officer	High	This will be reviewed as part of the IT Health Check in December 18. Once the health Check is complete actions will be taken to resolve issues identified, including and weaknesses around System Admin rights.	March 2019
5.	Update user profiles on the AD to ensure key information for all accounts is provided.	IT Client Officer	Medium	This needs to be done to enhance the functionality of O365.	April 2019
6.	Decommission Hart servers using unsupported software as soon as possible.	IT Client Officer	High	Plans are being developed to remove unsupported servers where possible. Some are tied into the 5C migration. The majority (7) will be decommissioned after 30 Nov 18, when the Revs/Bens system is turned off.	March 2019
7.	Carry out a PSN Assessment, ensuring an appropriate resource is available to assist where required.	IT Client Officer	High	Internal and external IT security health checks will be undertaken during December 2018. An action plan will be developed and implemented.	March 2019
8.	Review and update key IT Security Policies.	IT Client Officer	Medium	5C have recently agreed an approach to the implementation of council security	March 2019

				policies. They are currently being reviewed on a policy by policy basis	
9.	Establish an inventory of what IT devices have been allocated to each employee.	IT Client Officer	Low	Records should currently exist for all users. All mobile devices are now asset tagged as are desktops/laptops prior to being assigned to a user. These records will be reviewed and updated	March 2019
10.	Request confirmation from Capita that IT Assets are disposed of securely.	IT Client Officer	Medium	Processes for the safe disposal of equipment do exist and Hart follows the procedures that are carried out by Southampton CC. Confirmation will be sought and confirmed.	April 2019
11.	Continue data cleansing prior to migration to Sharepoint.	Heads of Service	Medium	The DPO reminded Heads of Service at Management Team in November of the need to continue data management work.	April 2019
12.	Ensure Capita are able to deliver effective continuity arrangements for the Councils IT Systems.	IT Client Officer	Medium	Continuity arrangements are discussed on an annual basis. The last meeting took place in Sept. I believe Capita meet this requirement but testing will be carried out.	March 2019
13.	Update virus protection on portable devices more frequently.	IT Client Officer	Medium	Virus protection is managed/monitored centrally by Capita. A more proactive	March 2019

				approach to mobile devices will be undertaken where the onsite engineer will actively ensure that devices that haven't been updated are put on the network. A reminder will also go out to staff to ensure laptops that are held in cupboards are logged onto the network. It must be remembered that any devices that access our network will have its patches installed immediately on connection.	
14.	Consider testing backup arrangements to ensure systems and data can be recovered.	IT Client Officer	Medium	Hart has a DR contract with a 3rd party supplier that is independent of Capita. System recovery and office space is available for testing. The issue is generally related to resources. The lead time to book the facilities can be up to 3/4 months for the testing slots.	March 2019