IT infrastructure reviews: key findings

Member audience analysis

Introduction

This document has been prepared by the Jisc enterprise infrastructure team of subject specialists to synthesise the infrastructure reviews undertaken by the team between late 2016 and 2020.

This version of the paper has been prepared for a general audience of Jisc members.

Data aggregation and narrative drafting have been undertaken by Rohan Slaughter, Jisc subject specialist (infrastructure systems and assistive technology). Marc Dobson, Jisc subject specialist (infrastructure applications) has undertaken data processing and additional data aggregation.

This document is structured thus, an executive summary is provided that identifies the key findings from this piece of work. We have used a narrative approach, in the form of an ‘exemplar infrastructure review report’ to provide further insights into the state of the infrastructure found across the Jisc membership. In constructing this section, we have used the same chapter structure as is used in the Jisc infrastructure review template.

Appendix A provides a summary of the core dataset that the analysis is based on.
Executive summary

• The Jisc enterprise infrastructure sub team has been carrying out the infrastructure review service since late 2016.
  - To date, 118 infrastructure reviews have been undertaken for Jisc members.

• Most infrastructure reviews have been carried out in the FE and skills sector, with a minority of HE members taking up the service.
  - We note that this may be due to the larger IT teams in HE organisations vs. their counterparts in HE means that FE colleges have a greater need for this service.

• The infrastructure review service is intended as a supportive process that seeks to enable service improvement.
  - The review is not an audit, it will only uncover what the Jisc member wishes to show the Jisc team. This means that the infrastructure review service is not a service that will seek to ‘find problems’ that a member does not wish to discuss. That said we can bring a fresh perspective to a Jisc member organisation to enable them to bring about service improvement.
  - We are also able to reference examples of good or best practice that we have seen work well in other Jisc members that may have already worked to bring about a given service implementation or improvement.

• We believe that we have seen the ‘middle range’ of Jisc members in terms of IT resourcing or IT / digital maturity levels.
  - Those with the greatest IT resource challenges perhaps may not wish to have this seen by an external party.
  - Additionally, those who are best resourced / most technologically mature may not require the service to the same degree as they do not perceive IT infrastructure to be a major concern.
  - We note that we have undertaken infrastructure reviews with Jisc members that represent both ends of this continuum.

• The most mature colleges undertake sufficient technology related strategic planning and ensure that the main strategic planning at colleges does include technology in such planning.

• A key finding is that where organisations have a CTO, CIO or head of technology type senior role that these organisations are able to make embedded use of technology due to improved organisation wide technology decision making that occurs in the right place and time to make a positive difference to service delivery.

• Most colleges find capital spending on IT infrastructure difficult.
  - The ongoing FE funding challenges have led to a large number of out of date core infrastructure systems continuing in use beyond their manufacturer or vendor end of support dates.
  - This creates a difficult cyber-security posture in a many of the organisations that we have worked with to deliver this service. Most colleges find managing the sustainable replacement or upgrade of both end user equipment and core infrastructure very difficult.
  - We have seen some innovative practice by IT teams that has enabled desktop and laptop fleets to have their lives extended through the fitting of new faster solid-state drives and additional memory, however this practice does have limits.

• Based on our analysis, IT support teams have been reduced in size in FE over the last two years in particular.
  - The average IT support staff to supported user’s ratio in general FE colleges now stands at 814:1, this is a substantial rise, and in our view too high to ensure a good quality IT organisation
  - In too many cases IT staff have left and have not been replaced.
  - In some cases, experienced and well qualified staff have left the sector altogether.
  - In most colleges, an IT skills shortage of some kind is reported, often as recent technical training has not been undertaken by IT teams.
In some cases, the skills shortage is down to the small size of technical teams. This concern is especially pronounced in sixth form colleges and in specialist colleges where the departure of even a single longstanding member of staff can result in serious difficulties for ongoing service provision.

We have met many highly talented and dedicated IT professionals when undertaking the infrastructure review service, who are most certainly a credit to the sector.

Our most popular ‘next step’ service following infrastructure review is the IT support skills assessment that aims to map the current IT teams skills and knowledge in order to identify key-person dependencies, to identify specific skills gaps and to identify any associated risks.

- Most organisations can improve elements of their networking provision (inclusive of WAN, LAN, WLAN, or telephony):
  - In most cases these concerns are down to a lack of capital investment over time.
  - A key finding in this area is that only a small minority of FE colleges have a resilient internet connection, this is a particular concern given the increased use of cloud hosted SaaS (software as a service) applications that the sector is now making use of.

- Servers and storage provision are also impacted by difficulties associated with capital funding:
  - This can mean that resilience is insufficient, or capacity is constrained.
  - For most colleges, the growth in the use of SaaS has not been matched by the use of IaaS (infrastructure as a service).
  - In most cases this is due to cost barriers or the view that locally provided systems are more appropriate to meet business needs.
  - It is our view that in almost all cases a hybrid model of both cloud and locally provided on-premises systems is the most useful option for FE colleges both in terms of cost-effectiveness and high-quality service delivery.

- There is scope for trust and identify services to be improved to give students and staff a seamless experience of accessing all the services and applications provided by organisations.
  - This can include a review of single sign on and access to externally hosted resources such as journals and other academic resources.

- Most colleges have moved email and calendaring to cloud services such as Office 365 and Gmail
  - Many colleges are making use of SaaS services to provide HR, finance, and other line of business applications.

- Device management can be improved in almost all cases:
  - Whilst the majority of colleges undertake Microsoft operating system and application patch management in a secure way, other third-party software management is often not as rigorously enforced.
  - Mobile device management (MDM) can be improved in most organisations that we worked with. Mobile phones are rarely managed by MDM systems, this may cause data protection concerns.

- Backup and disaster recovery preparations can be improved in most organisations:
  - In some cases, this is due to the age of systems, with them having been designed to mitigate against physical damage caused by fire, flood etc.
  - Such systems may not include logically or physically offline backups which in some cases can leave organisations without useful mitigations to recover from various common cyber-security threats such as crypto malware and bad actor / hacker attacks.

- Data and information security can often be improved using technical means such as mass storage policy enforcement, the use of compliance tools and through encrypting laptops and other mobile devices.

- Most of the organisations we worked with do not yet have cyber-security certifications in place such as Cyber Essentials, although most recognise the utility and usefulness of obtaining such certifications.

- The most mature IT organisations join up accessibility and assistive technology provision sufficiently with the IT team, this ensures there are no missed opportunities to improve support for disabled students.
Contents

Introduction ...........................................................................................................................................1
Executive summary ...............................................................................................................................2
An exemplar infrastructure review report ..........................................................................................5
  Strategic considerations .......................................................................................................................6
    How Jisc can help..............................................................................................................................6
  IT support ..........................................................................................................................................7
    How can Jisc help...............................................................................................................................8
Networks .............................................................................................................................................9
  How Jisc can help................................................................................................................................10
Servers and storage .............................................................................................................................11
  How Jisc can help................................................................................................................................12
Enterprise applications .......................................................................................................................12
  How Jisc can help................................................................................................................................13
Device management ...........................................................................................................................13
  How Jisc can help................................................................................................................................14
Security ..............................................................................................................................................15
  How Jisc can help................................................................................................................................16
Governance .........................................................................................................................................16
  How Jisc can help................................................................................................................................17
Appendix A: Infrastructure review synthesis dataset ........................................................................18
  Table1: Infrastructure reviews by Jisc member type........................................................................18
  Table 2: IT support staff ratios ..........................................................................................................19
  Table 3: Expected Cyber Essentials certification concern .................................................................21
Supplementary note ............................................................................................................................22
An exemplar infrastructure review report

In constructing this section, we have used the same chapter structure as is used in the Jisc infrastructure review template. Infrastructure review reports are constructed with a brief executive summary, a set of key points that include any relevant notes and where appropriate our recommendations to address the point.

We also include any proposed next steps that Jisc can assist the organisation with. These next steps often include the digital strategy review, and the IT support skills assessment. In fewer cases we offer the applications review service or the enterprise security review and risk assessment. We also provide strategic or bespoke consultancy inclusive of recruitment support and organisational design. Such next steps are only suggested where we feel the organisation will substantively benefit from them. Of the 118 infrastructure reviews undertaken to date a total of 64 of these ‘next-step’ consultancy offers have been taken up. This demonstrates a useful level of take up for these services.

In the majority of cases we provide an ‘appendix a’ that is based on the same chapter structure that is shown below in order for IT teams to backtrack as to why we have arrived at a particular key point or next step suggestion.

We use ‘Appendix A’ to provide further information for the IT than cannot be included in the main report. The main report is written for a general audience, whereas ‘Appendix A’ is of most use to IT teams.

This section is based on the data for general further education colleges, sixth form colleges, specialist colleges and land-based colleges. Where the collective ‘colleges’ is used it refers to these parts of the Jisc membership only. Other data has been omitted, inclusive of higher education organisations, institutes of adult learning and the performing arts colleges due to the small sample size for these types of organisation.

This section is formatted as an ‘exemplar report’ in order to highlight the best practice that we have found in the sector whilst undertaking this service.
Strategic considerations

- The most technologically mature colleges have a high-quality, integrated digital technology strategy.
  - The IT team are developing their infrastructure planning with direct reference to a wider organisational strategy or plan, inclusive of mapping to curriculum and other outcomes.
  - This ensures there is no disconnect between the work of the IT team and the other departments that they provide systems and services for.
  - Critical infrastructure investment is made based on the strategic planning to ensure that key priorities of the college are appropriately supported.
  - IT action planning is detailed and includes quality and impact measures based on the strategic plan.
  - Sustainability of IT infrastructure and other IT assets, inclusive of end user equipment is a key component that is addressed in such planning.
- The best performing colleges have a senior role dedicated to IT and technology such as a CIO, CTO, or head of technology type role.
  - Those colleges that do have this role generally have improved outcomes reported around the quality of technology services that are provided and how well they fit with organisational priorities.
  - Where high-performing colleges do not have this role a senior member of staff, such as an assistant principal, takes responsibility for line managing the IT team and champions technology related decision making at the senior level.
- The colleges with the highest levels of strategic fit between the IT team and other staff teams have a representative group of staff working with the IT team to help develop strategy and to prioritise the IT teams tactical work programme.
  - The requirements of the curriculum team are fully understood by IT teams through the input of this group.
  - We have seen evidence that this approach ensures that the IT team can prioritise resources or improvement projects in line with the wider requirements of the organisation.
- IT budget planning is well developed with replacement strategies for both end user equipment and core infrastructure.
  - The IT budget is considered within strategic planning, notably to support infrastructure renewal that is enabled by productive dialogue between IT managers, other mid-level, and senior leaders.
  - The IT estate is sustainable. IT teams know what they must replace and when, and senior leaders are supported to understand the urgency of these investment requirements so that they may be supported.
  - This point has increased in urgency due to the DfE / ESFA changes to the conditions of grant funding that require the Cyber Essentials certification to be in place from September 2020 and Cyber Essentials Plus to be in place for September 2021. In response to this driver, the colleges with the most developed strategic planning in place have scheduled for core networking, server or storage replacement and other critical infrastructure works to be undertaken in order to support the college to obtain Cyber Essentials certification.
- High performing IT teams have a good understanding of what their priorities should be and are able to articulate these clearly to the Jisc team at the start of the review.

How Jisc can help:

- The Jisc subject specialist team provide a digital strategy review offer as part of the consultancy service.
  - This service offer can assist colleges to develop their forward planning and can encourage colleges to consider the creation of a fully integrated strategic approach to technology.
- Through the infrastructure review service, we have been able to make representations to senior managers around the prioritisation of infrastructure renewal.
  - This has included supporting IT managers to present their concerns in an accessible or more easily understandable way that makes clear what the risks of not making an investment might be.
Note that this can include the identification of critical cyber-security issues, weaknesses with backup, restoration and disaster recovery or concerns around safeguarding that may impact inspection grades, or other staff and student related outcomes.

The Financial X-ray helps IT departments to benchmark, understand and easily compare overall costs. It is a useful tool to build a business case for changes in IT infrastructure and create an ongoing mechanism for dialogue between finance and IT departments. It can also provide a means of highlighting the comparative cost of shared and commercial third-party services.

**IT support**

- In the colleges that benefit from a mature IT organisation the support teams are well structured, with all staff members having clearly understood and well communicated roles.

- In larger colleges the IT teams are divided into sub-teams:
  - Operational or ‘first line’ support teams that provide direct support to students and staff.
  - A technical or advanced support team, who provide second or third line support. This group may also manage elements of the core infrastructure, especially in small to medium sized organisations.
  - In the highest performing colleges, a development group will build and test new systems and services prior to these being made available to the wider college community.
  - By separating out these roles the best colleges are able to ensure that service delivery is maintained in parallel to technical or development work.
  - Relationships between the IT team and allied teams are good, for example with MIS teams, LRC teams and others who provide technical support such as reprographics teams and audio-visual technicians or technicians that support digitally intensive subjects such as media.

- The most effective support teams in FE colleges are sized appropriately.
  - Where the support ratio of IT support staff to supported users exceed the 1:350-450 range we would expect to see examples of the IT team being under stress, we consider this to be an optimum range in most cases.
  - There are some cases where higher support ratios are sustainable, however in these examples the higher support ratios are only possible when the college has invested heavily in automation and systems management tools to enable a smaller number of team members to support larger numbers of staff and students.
  - In the highest performing colleges, the IT teams are of a size that matches the strategic goals of the college in terms of what the college is planning to achieve through the use of technology.
  - In the leading colleges, the management vision for the use of technology is fully matched by realistic staffing, both in terms of staff numbers and the skills base of the team.

- High performing IT staff teams are well led, by IT leaders who:
  - Have a wide experience base and critically higher levels of recent training.
  - Receive both leadership and management related development as well as technical training.
  - Have a clear understanding of the business of a college, both in terms of curriculum requirements and in terms of line of business functions.

- The skills base of the highest performing teams is broad and not held by particular individuals.
  - This enables teams to share core responsibilities such as security and reduces the number of key person dependencies and associated skills gaps.
  - Skills development and continuing professional development is mapped to the known training needs of the team, based on the identified systems and services that the team is providing to the college community.

- In the colleges where there has been sufficient (recent), high quality CPD made available to the IT team we see clear advantages over those colleges where this does not happen.
  - Where staff are supported and developed into their roles staff turnover may be lower.
- The IT team is well qualified and in the best examples, staff teams are well qualified with a range of both academic qualifications and IT vendor certifications.

- Training is not solely done online, rather this higher quality training may also be tutor led or classroom based, e.g. academic or vendor led (Microsoft, Cisco, VMWare etc. certifications) that allows improved collaboration and interaction with instructors and peers.

- Succession planning is considered carefully in high performing IT teams, this results in an absence of critical key person dependencies and skills gaps and generally higher morale which in turn leads to stable teams.

- Effective teams make use of software tools to prioritise tasks and time.
  - This can include a fully featured service desk software that enables staff and students to log support 'tickets'.
  - Service desk software is most effective in larger teams where such use is developed to include regular oversight of team member workloads and where metrics can be used to identify where tasks are 'stuck' for whatever reason.

- Reports from the service desk may be useful where data can be extracted to assist with management oversight and to maintain or evidence a KPI (key performance indicator). It is also possible to use this data to plan what equipment should be replaced based on analysis of failure rates.

- Colleges that use SLAs (service level agreements) will monitor this against KPIs, often using the service desk reports to evidence such. IT teams may find a service catalogue useful when managing expectations and ensuring that the IT team activities align with strategic objectives. Change control processes may also be useful to ensure high quality service delivery.
  - Where SLAs are in place, they include realistic response times and aid in planning IT service delivery.

- Where IT teams provide useful self-support materials to their user base such as making secure password reset tools, or a knowledge base available to staff and students that contains useful guides or other how-to material, this can reduce the burden on the first line support team.

- Proactive IT teams undertake appropriate systems monitoring and alerting in order to prevent systems or services from being interrupted by technical service outages.
  - This includes a proactive ‘daily routine’ that may involve physical inspections of locally held equipment, checking specific logs or alerts, and checking that automated tasks have completed such as backups or critical reports have been generated and supplied appropriately.

- Some smaller colleges find it useful to have access to a trusted third-party MSP (managed service provider) that provides some kind of third-line or advanced level IT support.
  - This support can help colleges with smaller teams access specific skills that it may not be possible to maintain internally due to resource constraints.
  - It can be useful to have a third party to call upon (as a backup to the local team), in the event that there is sickness or other issues causing absence, especially for smaller IT teams.

**How can Jisc help:**
- The infrastructure review service has routinely collected support ratio data since late 2016. In early 2018 the average support ratio for FE colleges was calculated to be 1:450 (IT support staff to supported users), we acknowledge that this figure was based on a smaller sample size than that now available to us, however two years later this has almost doubled to 1:814. This represents a substantial decline in the support available to students and staff.

- The ratios in sixth form colleges are lower at an average of 1:609. This should be taken into consideration alongside the point that the majority of SFCs are much smaller and the overall IT teams are commensurately smaller than their GFE counterparts. The support ratios in HE is typically lower, but as specified in the data section of these notes we do not have enough data on HE from this service to generalise further.

- The Jisc IT support skills self-assessment took kit provides an analysis of the overall skillset of an IT team. We supply you with with a matrix that lists all the skills required to run an IT organisation, this is customised to reflect the systems and service provided by your IT support team. Through team workshops the resultant
matrix is automatically colour coded to show at a glance where there may be skills gaps. New posts or professional development can be designed with the skills base of the current team in mind.

- The Jisc subject specialist team has also provided bespoke organisational design and recruitment support to Jisc members. This has included role design (role and person specification), interview question and task design and our specialists have also sat as recruitment panel members, notably when senior IT and technology roles are being recruited.

- Jisc also offers a range of technical and other training directly to our membership.

- Jisc has facilitated best practice sharing between Jisc members, this enables colleges and other organisations to see what has worked elsewhere and for exemplar organisations to share solutions with their peers.

**Networks**

- Having robust connectivity in place is now vital, especially as the majority of colleges have increased the number of remotely hosted or SaaS applications that they use.
  - This is an important concern as the majority of colleges have moved to SaaS provision of email and calendaring services, and also provide other line of business application software through ‘cloud-hosted’ means.
  - The increased use of SaaS means that the internet connection is one of the most serious ‘single points of failure’ in a college’s IT infrastructure.

- In colleges with multiple sites, the inter-site links are well specified to enable equity of IT service delivery over all sites.

- The colleges that have a truly resilient WAN (wide area network) link are well protected from service outages, should the secondary link be routed in a fully route-separate way. This means that the secondary connection shares no duct or active equipment with the primary connection.

- In the best examples of resilience colleges will configure BGP (border gateway protocol) to ensure that services gracefully failover from one internet connection to another, with no interruption to service.
  - In the majority of colleges that have a primary Janet connection the connection has sufficient bandwidth to meet their needs.
  - In a minority of colleges that have lower bandwidth 100Mbit/sec connections they are starting to find that this is insufficient at peak times, upgrades to 1Gbit/sec connections have been recommended to these colleges. Such upgrades are not currently fully funded.
  - Note that in order to have a fully resilient internet connection IT teams implement high availability pairs of firewalls or UTM (unified threat management) appliances to prevent these appliances from becoming a single point of failure.

- The most advanced colleges have a fully modernised WAN, LAN (local area network), WLAN (wireless local area network) and telephony system.
  - These colleges have a robust renewal or review pending of elements of LAN, WLAN, or other elements such as a telephony system.
  - In the best cases core network switches, WLAN controllers and wireless access points are under manufacturer support and are receiving regular security patches. This addresses key cyber-security concerns and means that organisations can meet the requirements of security certification requirements such as Cyber Essentials.
  - The most effective teams maintain LAN, WAN and WLAN diagrams and other documentation in order to reduce the time taken to troubleshoot issues and to plan improvements.
  - In the best examples network monitoring and alerting is proactively used to improve service delivery by monitoring traffic flows and to monitor up / down data on specific hardware or links. This means that IT teams can detect problems before they impact service delivery and allows teams to fix problems before they are informed that a concern exists by a user.
In the most secure networks comprehensive use is made of VLAN structures to appropriately segregate types of network traffic, this improves security and limits the damage that specific threats such as malware or bad actors may cause.

In the most resilient networks, the core is structured as a resilient ring, allowing a break in the ring to be mitigated by alternate routes to all distribution points. In addition, distribution switches are multi-homed so that they connect back to two or more core switches that provide connectivity to the rest of the network.

Most modern networks operate with at least 10Gbit/sec on the core and 1Gbit/sec to all endpoints.

In terms of wireless networks (WiFi) modern networks use the 802.11ac standard or newer to provide high density, high bandwidth service delivery.

Wireless Access Points (WAP’s) are located in accordance with the construction of the building in order to eliminate dead spots, and to provide a high level of service delivery. The IT may have optimised the placement of access points using a wifi design tool such as Ekahau.

Wireless networks perform best when the number of network names (SSIDs) are as low as possible, in the best examples the IT team use a RADIUS technology such as eduroam to enable users to be dropped into different VLANs based on group membership rather than having to advertise multiple SSIDs.

BYOD (bring your own devices) support can be robustly provided through the use of wireless profiles, such as those made possible by eduroam and similar systems. Alternatively, a captive portal can be used to force users to authenticate using their organisational account. Without such systems in place it is not possible to provide accountability through resolving all web traffic to an individual user.

Guest access is highly controlled, either through issuing a specific account to users as guest users sign into the building or through the use of a system such as eduroam for authorised visitors.

All wireless networks are encrypted to prevent a ‘man in the middle’ type attack from being used to access college data.

Effective facilities are in place to enable wireless devices to present using available large format screens or projectors.

• Access to services from offsite is provided through a secure method that mitigates against personal data being exfiltrated. For example the college may provide a VPN (virtual private network), perhaps using a technology such as Microsoft Direct Access, or will provide a VDI (virtual desktop infrastructure) that enables staff and possibly students to securely access a desktop that is hosted internally on the college’s systems.

• The most digitally mature colleges have useful web filtering, monitoring, reporting, and altering services that meet the specific best practice expectations of Ofsted around good safeguarding practice, especially in the context of the Prevent Duty.
  - In these cases, all web traffic generated from all endpoints, inclusive of managed devices, shared devices such as iPads and BYOD devices are attributable to the individual user account to provide full accountability.
  - All traffic is filtered, monitored, reported on and proactive alerting is in place for all safeguarding related concerns.

• Telephony is based on modern VoIP (voice over internet protocol) technology that enables calls to be routed over the internet rather than via antiquated (and soon to the withdrawn) services such as ISDN30.
  - In the best examples full unified communications systems are deployed that make use of the concept of ‘presence’ (call the person and not the desk), in order to leverage technologies such as softphones or divert to mobile.

How Jisc can help:

• Jisc provides a range of connectivity services associated with the Janet Network, the UK’s NREN (national research and education network).

• The eduroam service provides users with authenticated network logon and access to the internet through a single wifi profile and set of credentials, wherever the service has been made available by participating organisations. Connection can be seamless and automatic. Wired connections can also be supported.
• The Jisc subject specialist team provides bespoke 1:1 guidance around networking elements as part of infrastructure review. This can include suggestions around LAN, WLAN, or telephony improvements.

• As part of the review of web filtering, monitoring, and reporting in the context of safeguarding practice, the team have provided appropriate support materials:
  - We have provided specific remediation guidance in line with the Ofsted thematic review ‘how well are FE and skills providers implementing the Prevent Duty’.
  - The Jisc paper Web Filtering and monitoring: guidance for the further education and skills sector in the context of the Prevent Duty is hosted on the ETF Prevent for further education and training microsite.

• Jisc provides a range of telephony services:
  - It is possible that a cost saving may be achieved using Page One’s JanetTxt system to send SMS.

Servers and storage

• The vast majority of colleges have virtualised their on-premises server infrastructures. The effective use of virtualisation means that the total hardware footprint has been reduced in most cases, with a small number of server hosts running a virtualisation hypervisor that in turn runs a number of virtual servers.
  - Virtualisation is a useful technology as it abstracts the services from the hardware on which they run, it also makes backup and restoration faster and more reliable.
  - The most mature colleges have sufficient compute resources, notably the best colleges ensure that an element of the can system fail, and there continues to be sufficient compute to manage without disruption. This means that all systems and services can stay online, should any one host fail.
  - The best colleges ensure that server virtualisation systems continue to be kept up to date, this ensures that future virtualisation and operating software updates will be supported by the hardware.
  - In the best cases, compute (server host) hardware is fully under manufacturer support and can support current virtualisation software or server operating systems.
  - The most secure IT operations only use fully supported server operating systems and have eliminated any legacy systems or applications that only run on older operating systems.
  - The most advanced examples include development or testing environments to allow IT teams to test new systems or services or to simulate upgrades and other large-scale changes of systems prior to applying such to the production environment.
  - In the best examples server room contingency is outstanding with redundant UPS (uninterruptible power supplies), air conditioning and fire detection and suppression systems in place. In addition, the most resilient organisations include environmental monitoring and alerting inclusive of temperature and moisture sensors.
  - Again, the most advanced server rooms are physically secure with good use made of electronic access control systems to both control and log access in place. In addition, CCTV systems or master key systems may also be used.

• Most colleges have sufficient storage capacity, the best plan to ensure that future growth can be accommodated alongside considering how to support media courses and other curriculum areas that make greater use of storage over other courses.
  - In the best cases storage is being proactively managed to ensure that archiving and retention policies are enforced. In the most outstanding examples data protection officers are actively engaging with IT teams to ensure that policies are being technically applied.

• The most resilient organisations make use of an active – active cluster with at least two main server rooms that are sufficiently specified to run the entire college enterprise from either location should one be compromised.

• Alternatively, some colleges have chosen to implement a DR (disaster recovery) environment that would enable a sub-selection of vital systems to be run from a smaller infrastructure whilst the primary systems were brought back online. This is noted to be a less costly option over an active - active arrangement.

• We note that take up of public cloud hosted IaaS is very low.
We understand that this is down to IT managers determining that it is generally not cost effective for most FE colleges to make effective use of IaaS due to scale, high cost, and limited connectivity arrangements such as not having a resilient internet connection.

Also, due to the specific use case of college based systems such as the fast storage or low latency required by media-based courses such as games design, photography etc.it is not in all cases, appropriate to make use of offsite storage as this could result in poor performance.

It is important to note that whilst IaaS use is very low, SaaS applications are in increased use as is explored in section the Enterprise applications section below.

How Jisc can help:

- The infrastructure review service has enabled IT teams to understand how to upgrade or improve existing compute and storage systems in order to make the best of what equipment is already available or to make useful decisions about where to target future investment.
- The applications review enables the future infrastructure requirements to be well understood by the team so that applications may be provided from a SaaS, or on-premises method.
- Most colleges have already moved core applications to SaaS delivery, however there are a number of opportunities to streamline service delivery, such as trust and identify management and single sign on, and these have been highlighted through the infrastructure review service.
- The Jisc cloud consultancy service offer enables colleges and other organisations to obtain support to move applications and other systems from on-premises to cloud service provision.

Enterprise applications

- In the vast majority of colleges email and group calendaring is provided by Microsoft's Office 365 service.
  - In a minority of colleges email is provided using a Microsoft Exchange server on premises
  - A small minority of colleges are using Google Gmail as part of the G Suite for education.
  - Our research shows that other email services such as Novell Groupwise on-premises servers have been all but eliminated.
  - However, our research also found that some organisations use Microsoft Office 365 alongside Google services, although fewer use the email services from Google when using both leading SaaS suites.
- Email, calendaring, and related services are critical to the operations of all Jisc members:
  - In the most mature organisations, we see IT teams deploying mailbox archiving to ensure that staff mailboxes can be retained, this technology enables FOI (freedom of information requests) to be met and facilitates general data retention.
  - In the most secure scenarios, we see IT teams making use of mail washing technology to reduce the chances of phishing emails, malware, poisoned links, or dangerous attachments being introduced into college systems.
  - We also see effective use of compliance tools such as the Office 365 compliance centre being used to limit opportunities for personal data leakage or deliberate unauthorised data exfiltration.
  - The most mature organisations couple technical measures with effective user training on managing cyber-security, data protection and other critical points.
- MIS (management information systems) applications are primarily provided by a small number of companies (inclusive of OneAdvanced (Compass), Tribal’s EBS and Capita’s Unit-e).
  - We have not seen any clear sub-sector or regional pattern in their use, nor can we identify a clear market leader.
- A small minority of colleges are utilising MIS systems that have been developed in house.
Where this is the case the development teams have built impressive levels of integration with other systems and have also built data warehouses or other high-level services that are used by multiple applications.

We note that there is potentially an opportunity to consider how this specific sector expertise could be shared with other Jisc member organisations.

- **SaaS (software as a service)** is now in widespread use in colleges to provide HR, finance, and other lines of business applications.
  - Where colleges not already making use of SaaS for their core applications, most colleges are considering using this technology, this can be useful as it reduces the requirements for local hardware to provide services.

- **Very few colleges have local enterprise architecture services inclusive of a data warehouse.**
  - These services are only found in a very small number of colleges and are often a feature of colleges that utilise an internally developed MIS system and have access to a skilled internal software development team.

- **In most colleges student facing applications typically include a VLE (virtual learning environment), LMS (library management system) and e-portfolio systems, notably where colleges are providing apprenticeships.**
  - A minority of colleges offer students bespoke applications or portals that can be accessed from a variety of devices, inclusive of mobile devices.
  - The maturity of online learning services varies greatly, as has been highlighted by the COVID-19 pandemic. In most cases there are few if any dedicated e-learning staff, and where these posts do exist, they are rarely located in the IT team.

**How Jisc can help:**

- **The Jisc applications review can help organisations to identify applications that may be end of life, or otherwise need to be replaced. It is also possible that a number of older applications can be replaced by a single application, this can bring improved integration a greater cost efficiency. An application review can also assist IT teams to size their future infrastructure appropriately as a greater use of SaaS services is made.**

- **The software procurement services provided by the Chest service are likely to bring about a substantial cost saving for Jisc member organisations.**

- **Cloud professional services. Take advantage of our hands-on cloud capabilities, to solve a range of short-term and long-term challenges.**

- **Our learning analytics service helps you put your data to work to tackle some of the big strategic challenges – and we will support you every step of the way. It is the world’s first national learning analytics service developed to address the key strategic goals of HE and FE organisations.**

**Device management**

- **Most colleges have a mix of Windows desktops and laptops.**
  - Most colleges have a mixture of Apple Mac OS X desktops and Windows PCs, however in almost all mixed installations the Windows machines vastly outnumber the Apple Macs.
  - Where Macs are used, they are often joined to or managed by Active Directory and are managed by automated tools.

- **Tablets and other consumer grade ‘appliance’ equipment is in use, but this trend has declined:**
  - Interestingly many colleges that have deployed tablets or ‘appliance’ grade devices such as Chromebooks are reversing these decisions and are instead deploying Windows laptops. In some cases, this revision to policy has been down to utility or performance problems, in others it has been related to management or compliance concerns.

- **The most mature IT organisations make use of automated tools such as SCCM (System Centre Configuration Manager) or MDT (Microsoft Deployment Toolkit) to deploy operating systems and software.**
- A minority of colleges use other tools, such as device imaging, this is a useful finding as we would consider such tools to be obsolete.
- A small number of colleges have started to use cloud-based management tools such as Microsoft Intune, although such tools are rarely used to manage desktops or laptops (within a campus LAN) that are running Windows 10.

- The majority of colleges use WSUS (Windows Server Update Services) or SCCM to patch Windows endpoints inclusive of desktops, laptops etc.
  - The minority of colleges do not utilise such automated management tools, this results in a difficult cyber-security posture as patches are not applied in a timely manner and IT teams cannot be certain that all endpoints are fully patched against various security risks.
  - In some cases additional effort is expended to ensure that college owned laptops are patched, in these cases the effort is useful as users benefit from secure machines that are more usable, as they do not waste users time when critical updates are required prior to use.

- It is useful to identify that the majority of colleges use WSUS or SCCM to patch servers, or IT teams carefully manually patch servers.
  - In some cases, critical servers are manually patched, and less critical services are patched using automated tools. All of these options are reasonable so long as the management of critical and important security patching is approached systematically.
  - The minority of colleges do not patch servers in a timely fashion, this is resulting in a very challenging cyber-security posture where data protection and operational security present a high level of risk for organisations.
  - In most cases where colleges do not follow the expected best practice around patch management this can usually be linked to having a smaller than expected IT team, or in a minority of cases to a lack of recent technical training for the team.

- In the most mature organisations third party software patching is not overlooked, unfortunately in many cases this area of security patching is not fully addressed.
  - In some cases, this means that applications provided by software companies other than Microsoft may be patched rarely or simply not at all. This could lead to critical software vulnerabilities potentially being exploited by malware or bad actors (hackers).

- The best performing colleges have a mature MDM (mobile device management) system to manage iPads and other mobile devices.
  - Very few colleges use an MDM to manage corporately owned mobile phones.

- Most colleges use WEEE approved recycling services to ensure that devices are properly disposed of and that data protection policy is maintained.

- Microsoft software licensing is routinely provided by EES agreements that are now replacing the previous Campus volume licencing agreements.

- Most colleges are encrypting laptops and other mobile devices.

- The minority of colleges are actively technically controlling the use of removable storage, this means that flash drives and other similar devices could be used to exfiltrate data, creating a potential data protection concern.

- Most colleges can improve some aspect of device management, whilst this is mostly about improving security or data protection it is also about ensuring a high quality and consistent user experience.

How Jisc can help:
- The Jisc infrastructure review service can often highlight device management best practice improvements; indeed, few reviews do not highlight at least some of the points made above.

- The Chest agreements include Microsoft EES agreements and are a useful way of ensuring best value when procuring software.
Security

- In the most mature organisations the IT team is sufficiently able to ensure that all security related tasks may be handed off to another member of the team, this both enables IT team members to have a genuine break from their duties and reduces the chances that an internal bad actor will go unnoticed.

- In a minority of cases we see write once logging or remote system logging in use, the use of this technology means that those with administrative access cannot delete or tamper with the system or security logs. We note that colleges can consider implementing these technologies, especially if making substantial use of contractors.

- It is useful to note that in the vast majority of colleges limited (standard) user accounts are used by the IT team for the bulk of their work. In these instances, administrative accounts are only used for tasks that require this access. We note that this account management method limits the exposure (and therefore the risk of compromise) of the domain administrator and other administrative accounts.

- Only in the most digitally mature colleges that have sufficient resources to plan, rehearse and revise their backup / disaster recovery processes do we see fully documented and rehearsed business continuity processes.
  - This point is directly linked to the small size of most college-based teams who rarely have the time for proactive measures such as disaster recovery planning.

- Perhaps most concerningly, many organisations have no form of logically or physically offline backup systems, meaning that we often make strong suggestions about improvements in this area as the lack of offline backups is a critical cyber-security resilience point.
  - This is partly as some colleges have retired offline tape backups or removable disk pack backups in favour of ‘online’ backups that some perceive to be ‘more modern’, however offline tape backups are still a valid and cost effective mitigation against various cyber threats inclusive of crypto-malware.
  - Where colleges do have logically or physically offline backups the majority of colleges have not invested in offsite (cloud hosted), verified logically offline backup systems, as this option can come at a high cost.
  - Offline backups such as tapes or removable disk packs are a useful mitigation in the event that both primary systems and online backups are destroyed by the same bad actor (hacker) or malware incident.
  - Most backup systems have been designed with a different, historical or legacy risk profile in mind, meaning that in most cases the provision or contingency against a physical event (fire, flood or catastrophic hardware failure) is far better developed than the provision aimed at guarding against or recovering from a cyber-security incident.
  - Unfortunately, cyber-security incidents are perhaps more common than a physically destructive event.
  - With most colleges failing to have a logically or physically offline backup to mitigate against damage caused by bad actors (hackers) or malware outbreaks we would link this point to the difficulty that some colleges have with timely infrastructure renewal, which we identify as being down to high cost.

- Only the most developed IT organisations have the resources required to implement a disaster recovery environment, this means that in most cases following a disaster the RPO (recovery point objective), as in the time taken to restore systems following an incident, will be governed by equipment lead times.

- The RTO (recovery time objective), as in the maximum amount of time over which data might be lost, is generally good in the event of a physical event, however in the event of a cyber-security incident the RTO could be highly variable, in that without offline backups there may be no viable restoration route for locally held systems.

- It is useful to identify that the majority of college firewalls are modern, kept up to date with security patches and include security subscriptions such as gateway anti-virus and intrusion detection or intrusion prevention signature updates.
  - Most colleges also use their main firewall appliance (sometimes this is referred to as a UTM, unified threat management appliance) for web filtering, monitoring, reporting, and alerting.
  - A small number of colleges make use of a dedicated web filtering, monitoring, and reporting appliance in addition to the main firewall.
- A smaller number of colleges use ‘e-safety’ software such as e-safe or Impero that use approaches including keystroke logging to enforce safeguarding policies.

- Most colleges are generally compliant with the best practice expectations of Ofsted in relation to the Prevent Duty and good safeguarding practices.
  - The minority are not compliant and may find this challenging at Ofsted inspection, should this area be considered in detail by the inspection team, for more information on this point refer to the ETF Prevent Duty resources and to the Jisc document ‘Web filtering and monitoring: Guidance for the further education and skills sector in the context of the Prevent Duty’.

- The physical security of IT assets is generally good with server rooms and other key areas such as comms rooms secured by access control systems, master key systems and CCTV.

- Physical protection or contingency of server rooms is generally good with fire detection systems, dual air-conditioning systems, and UPS (uninterruptible power supplies) in common use.

- Only a minority of college server rooms have fire suppression and environmental alerting systems in place meaning that few colleges have a tier 1 datacentre status.

How Jisc can help:
- As described above most infrastructure reviews reveal that improvements are often required around the cyber security posture of organisations, this is primarily linked to mitigations around disaster recovery and business continuity but also includes other practice based cyber-security improvements.

- The Janet network includes a high level of in-built cyber-security protections such as Foundation DDoS mitigation, which mitigates against the effects of distributed denial of service attacks.
  - Jisc provides a range of cyber-security services inclusive of the CSIRT (computer security incident response team), the phishing framework and the penetration testing service.
  - The cyber security assessment service may also be useful to organisations that required a holistic assessment of their cyber-security position.

Governance

- Most colleges can improve elements of their AUPs (acceptable use policies), notably around the safeguarding / Prevent Duty points discussed above.

- The majority of colleges do not have security certifications such as Cyber Essentials in place.
  - This is a specific concern given the changes to the ESFA conditions of grant funding contract.

- In the majority of college-based IT teams have a lower awareness of accessibility and inclusion matters:
  - We note that this is again likely to be a function of the small size of some college-based IT teams
  - This limited support for assistive technology and / or accessibility could lead to a number of difficulties, notably around the application of the Equality Act, due to the anticipatory duty to meet the needs of disabled people as proscribed by the Equality Act.
  - However, in most cases, colleges move to improve this point when it is discussed in the infrastructure review if it has not already been addressed, for example by implementing portable desktop customisation for user’s accessibility settings, using a technology such as UE-V (user experience virtualisation, FSlogix Profile Container) or providing ‘roaming profiles’ on request, or universally.
  - We also note that in most cases IT teams express the view that accessibility or assistive technology generally is ‘not their responsibility’, instead pointing us to the ALS (additional learning support) teams.
  - Very few colleges have a dedicated assistive technology role, and where they do this post is rarely located in the IT team.
How Jisc can help:

- Jisc subject specialist for technology and the law (John Kelly) is available to support Jisc members with legal matters pertaining to technology use.
  - Colleges may find the updated Jisc guide 'records retention management' useful in developing policy and practice around data retention standards.

- Jisc now offers a trusted way to gain and renew Cyber Essentials certification, helping to make sure vital security precautions are in place.
  - Jisc offers a Cyber Essentials drop-in clinic to Jisc members in preparation for supporting members to achieve both Cyber Essentials and Cyber Essentials Plus.
  - Further information is available from the IASME consortium, notably the self-assessment questions.

- Jisc offers a range of support on assistive technology and accessibility.
  - Jisc subject specialists are actively representing members requirements and views at various assistive technology and accessibility national forums such as the APPGAT (all party parliamentary group for assistive technology) and the DfE’s EdTech unit’s AT experts’ group.
Appendix A: Infrastructure review synthesis dataset

Table 1: Infrastructure reviews by Jisc member type

A total of 118 Jisc infrastructure reviews undertaken from late 2016 to early 2020

<table>
<thead>
<tr>
<th>Type of Jisc member</th>
<th>Count</th>
<th>% of sub-sector</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>General further education college</td>
<td>59</td>
<td>27.8</td>
<td>All FE colleges across UK</td>
</tr>
<tr>
<td>Sixth form college</td>
<td>18</td>
<td>35.3</td>
<td>Six form England only</td>
</tr>
<tr>
<td>Higher education</td>
<td>10</td>
<td>6</td>
<td>All HE orgs UK wide</td>
</tr>
<tr>
<td>Specialist college</td>
<td>21</td>
<td>16.8</td>
<td>England and Wales only</td>
</tr>
<tr>
<td>Land based college</td>
<td>5</td>
<td>38.5</td>
<td>England only</td>
</tr>
<tr>
<td>Institute of Adult learning</td>
<td>3</td>
<td>30</td>
<td>England only</td>
</tr>
<tr>
<td>Performing arts</td>
<td>1</td>
<td>50</td>
<td>England only</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
<td>n/a</td>
<td>This applied to a membership body</td>
</tr>
</tbody>
</table>

The number of infrastructure reviews has varied by sub-sector. By far the greatest number of reviews (59) have been undertaken in General Further Education (GFE) Colleges. With almost 28% of the entire GFE sector having undertaken the service we believe this is a representative dataset.

Sixth form colleges have a smaller number of reviews (18) but a greater percentage at just over 35% of the sector having received the service. As such we feel this is a useful dataset.

A small number (10) of Higher Education (HE) organisations representing only 6% of the sector have received the service, as such we do not think this is a representative dataset and would caution against any generalisations being drawn from such a limited sample.

We have generally only worked with the larger, longer established specialist colleges, almost all of whom are members of the membership body for the specialist colleges, Natspec (the national specialist colleges association). Only 41 specialist colleges are Jisc members, the remainder are not Jisc members due to historical funding arrangements. In recent years, many smaller specialist colleges have been created, these include specialist school sixth forms and very small private providers that may only have 10-15 students or less. This dataset is therefore representative of the larger, longer established Natspec specialist colleges that are members of Jisc. From this perspective we have worked with half of such colleges, the dataset is therefore valid for this group, if not the smaller, more recently established specialist colleges.

We have worked with 5 (38.5%) land-based colleges, the dataset is therefore useful. We have worked with a small number of the institutes of adult learning (3) representing ~30% of the sub-sector, this data set is not thought to be useful to draw generalisations from as the colleges in this group are highly varied in their nature. The one organisation in the ‘other’ section refers to an adult organisation, we have discounted it from our calculations as it is not comparable to any other organisations covered by this work.
Table 2: IT Support staff ratios

The support ratio (supported users to IT support staff) is calculated by taking the total number of supported users (staff and students) and dividing this by the number of IT support staff available. Note that part time staff are counted as ‘1’ as they typically require similar input from the IT team as a 1.0FTE member of staff.

<table>
<thead>
<tr>
<th>Support ratios</th>
<th>FE colleges</th>
<th>Sixth form colleges</th>
<th>HE</th>
<th>Specialist colleges</th>
<th>Land based colleges</th>
<th>Adult Learning</th>
<th>Performing Arts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lowest</td>
<td>314</td>
<td>300</td>
<td>166</td>
<td>96</td>
<td>384</td>
<td>1063</td>
<td>307</td>
</tr>
<tr>
<td>Highest</td>
<td>2767</td>
<td>1180</td>
<td>428</td>
<td>500</td>
<td>868</td>
<td>1932</td>
<td>307</td>
</tr>
<tr>
<td>Mean</td>
<td>814</td>
<td>609</td>
<td>302</td>
<td>227</td>
<td>612</td>
<td>1439</td>
<td>307</td>
</tr>
</tbody>
</table>

Further education

The support ratio for general further education colleges has gone up substantively since we last aggregated the data. At the end of 2017, the average (mean) range for FE colleges was 1:450 (note that this was calculated with a smaller sample size), this means that the average has almost doubled over ~2 years. We have anecdotal evidence that as IT staff are leaving FE colleges they are not being replaced, but rather are being seen as a cost saving measure.

It is noted that once the support ratio goes above approximately ~500:1 (supported users to IT support staff) we see difficulties in providing a sufficient skills mix in the team, difficulty in covering staff absence or leave and in some cases critical service failures. It is therefore alarming that the average ratio figure has gone up so rapidly. We also recognise that it is possible to run an IT support service with a higher support ratio where there has been a substantial investment in IT automation tools, however it is difficult to spend the time configuring such tools if such an investment is not accompanied by time from contractors or vendor staff members to provide configuration support or training to the local IT team at the initial setup and hand over stage.

We are very concerned about the high support ratio figures for FE colleges. There is evidence from the review dataset to show that in some cases the most experienced IT staff are leaving FE for roles in other sectors. This has left teams depleted and in some cases being led by the few staff who remain, some of whom may have fewer qualifications and less experience. This loss of experience is a substantial risk to continuity of service delivery.

This grave situation is not universal, we have also met some very well qualified staff who are working hard to maintain service delivery, even with much smaller teams than they previously had access to. It is a concern that IT service teams have, (alongside other support services within FE colleges) been reduced in this way. It is recognised that whilst this is as a result of the funding reality facing FE colleges it is still a serious concern to IT organisations. We note that the best performing FE colleges have a senior member of staff responsible for technology areas, this role is often a CIO (chief information officer), CTO (chief technology officer) or head of technology type role. In some cases, an assistant principal is allocated the role. In colleges where the IT manager reports into another service function head, such as the head of estates, finance or other areas, IT service quality is generally less favourable. We base this conclusion on feedback from a range of staff from general FE colleges.

Sixth form colleges

The data for sixth form colleges is similar to GFE, although the support ratios are lower in all three categories. The average is still high but is usually manageable. We note that in most sixth forms staff are less experienced and have fewer qualifications vs. their counterparts in GFE colleges. This may be a function of scale, where it has not been possible for smaller SFCs to match the investment in training made by GFEs. As SFCs tend to be overall smaller than GFES we note that the skills mix required to run an IT organisation is harder to maintain in what are smaller IT teams in terms of absolute staff numbers. As with GFE colleges there is some evidence that IT staff are leaving and not being replaced, and this is leading to some of the least experienced, less well qualified staff remaining in service. As with GFES this can lead to IT service difficulties in SFCs.

Higher education

Whilst we believe the HE dataset is too small to derive useful generalisations from we do note that the support ratios in HE are much lower than for GFE or SFC. This reflects the generally higher levels of funding in HE.
Specialist colleges
Specialist colleges have a higher staffing density than SFC and GFE due to the nature of the support needs of their students. This higher staffing density has translated into lower IT support ratios overall. In some cases, specialist colleges are very small, and the lower support ratio may translate into an IT team of 1 or 2 people, and this can lead into very serious continuity or succession planning problems when a single member of staff leaves a college. We note that service continuity and the skills mix to maintain an IT organisation are more acute problems in specialist colleges than most GFE colleges. The impact of a single member of staff leaving has in some cases reversed years of IT progress due to the level of site specific or cohort specific ‘embedded knowledge’ leaving with some key members of staff.

It should also be noted that the level of assistive technology (AT) related knowledge in some specialist colleges is far lower than expected. In most cases the IT team does not provide direct support for AT, rather that work is done by the education or therapy staff teams. We note that this AT / IT disconnect often leads to service difficulties for students and staff. In the highest performing specialist colleges, there are good links between IT and AT support staff and with the education and therapy teams. In the best performing specialist colleges, a senior member of staff has responsibility for all technology related areas, inclusive of AT, IT infrastructure and e-learning.

Land based colleges
The dataset for land-based colleges is a small number (5), but a large percentage (38.5%), it is therefore thought to be useful. The support ratio for this group of colleges is lower than both GFE and SFC. The land-based colleges tend to be smaller than GFEs and have commensurately smaller IT teams. The succession planning and skills mix concerns we have noted for both SFC and SC apply to the land-based colleges.

Institutions of Adult Learning
We do not believe that we have a useful data set for the IoAL group. The support ratios are very high in this group, which may reflect concerns with the level of funding such organisations receive. It is noted that in almost all cases we had concerns about succession planning, training, and the resulting resilience of the IT teams in this group of colleges.

Performing arts
As this is a dataset consisting of only one college, we do not believe it to be useful to attempt to draw out any conclusions.
Table 3: Expected Cyber Essentials certification concern

Across all member types the majority of the organisations we worked with had an expected Cyber Essentials certification concern. We arrived at this conclusion by looking at the security related key points found through the infrastructure review process. We then identified those organisations that had older equipment, software, or difficult cyber-security practice evident that would result in a failure to attain the certification.

<table>
<thead>
<tr>
<th>Jisc member type</th>
<th>Cyber Essentials concern present</th>
<th>No Cyber Essentials concern</th>
<th>Cyber Essentials concern unclear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Further education college</td>
<td>44</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>Sixth form college</td>
<td>16</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Higher education</td>
<td>8</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Specialist college</td>
<td>19</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Land based college</td>
<td>4</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Institute of Adult Learning</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Performing arts</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

We note that in most cases substantial capital investment is required to remediate these concerns. In the case of FE and skills the problem is compounded by the ESFA conditions of grant funding requirement that has now mandated all colleges in receipt of ESFA funding must have Cyber Essentials in place by September 2020 and Cyber Essentials Plus by September 2021. We also understand that ISO27001 certification will be required at some future point. Based on our infrastructure review dataset we expect that it is not possible for these deadlines to be met by most colleges.

Further information on this requirement is provided within the ESFA Update further education: 29 January 2020. In order to address this point, we suggest that in the case of FE members that ringfenced infrastructure funding should be reinstated in order to address the concern of aging core infrastructure. This could be done in a similar way to the previous system that mandated an ILT strategy and planning development programme. The table above shows the level of Cyber Essentials certification concern by member type.

We note that in most cases the reason for the concern was borne out of a lack of modern infrastructure equipment (servers, storage, core network hardware etc.) that are capable of running a current software / firmware version and may not be supported by the vendor. In some cases, members were running out of date server operating systems or desktop operating systems, thereby presenting a substantial risk. In other cases, we had a concern around service practice, such as administrative password management or the server, desktop operating systems and software patch management approaches.
Supplementary note

Jisc cannot be held responsible for the content of third-party sites linked to from this document.

All information provided here is provided on an “as is” basis and is for general information only, unless the information is part of specially contracted work, in which case the terms of the corresponding contractual agreement between us shall apply. Whilst we apply a wealth of collective knowledge and experience to ensuring the accuracy and completeness of our advice and of the information we provide, we are unable to provide any representations, warranties or guarantees, whether express or implied, as regards this advice and information. It therefore remains the responsibility of the Jisc member to ensure that they consult with all relevant roles and groups within their organisation, and take their views into consideration as appropriate, before acting upon any of the supplied advice or information.