<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>3</td>
</tr>
<tr>
<td>IT Risk Universe</td>
<td>5</td>
</tr>
<tr>
<td>2020 Technology issues for the Education sector</td>
<td>6</td>
</tr>
<tr>
<td>Emerging technology issues for the Education sector</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

The Education sector continues to undergo significant transformation with huge opportunities, however this comes with increased risk.

Technology is playing a larger role than ever before in all aspects of higher education, from administrative processes to student education, and as a result it is no surprise that industry leaders often rank IT-related risks towards the top of their concerns.

Our CIO survey 2019, conducted with Harvey Nash, identified that almost three-quarters of IT leaders reported they are making moderate or significant investment in IT with investment in mobile technologies not far behind.

Greater investment comes with a number of opportunities but also presents greater risks.

In the last 18 months we have seen risks and opportunities related to IT systems and the adoption of emerging technologies throughout the Education sector. For example:

- A London based Russell Group University breached the General Data Protection Regulation after sharing a list of people's data with the Police without a legal basis to do so.
- A report into the effectiveness of information security controls, published by Jisc (formerly the Joint Information Systems Committee) and the Higher Education Policy Institute (Hepi), had a 100% success rate in getting through the cyber-defences of higher education institutes.
- There have been a year-on-year increase in the number of University-related phishing attacks which appear to have harvested credentials for university webmail services with the possibility of these being linked to the Student Loans Company-related attacks.
- In the Higher Education Overview report published in January 2019, the ICO identified that only 25% of the 16 Universities tested had an adequate Information Security policy in place, only 31% had a Incident management policy and only 19% had an effective way of communicating the policy to staff.

The Department for Education published its Strategy for Education in the summer of 2019 and highlighted the potential for the sector to grow and flourish through the use and development of technologies such as cloud.

However, the potential to utilise such technologies is dependant on adequately mitigating system and control weaknesses related to data privacy, legacy IT infrastructure, and a lack of technical capacity and capability within the workforce.

Penetration testing conducted over a sample of Higher Education institutions had a 100% failure rate

As reported by Jisc and Hepi in their Information Security Controls report

© 2020 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
Executive Summary

We have provided an analysis for nine key risks we have identified specifically for the Education sector.

These are Data Privacy, Cloud Implementation, Cyber Security, IT Infrastructure, Budget Restrictions, Service Desk, De-centralised IT, Data Governance and Legacy IT.

These risks are based on research and our experiences with clients in the sector over the past 12 months. We feel that these risks should be considered as part of Higher Educations and Universities’ risk management programme for 2020/21.

Only 31% of Universities sampled had documented Incident Management Policies & Procedures

ICO Higher Education Overview report published in January 2019

Within this document, we have used our industry experience and our understanding of a wide range of technology and applications to produce a heatmap of IT risks we believe are most relevant to Education providers, and should be closely managed.

We have provided a focus on nine specific key trends in IT which we believe are key in 2020 throughout the Education sector. For each of these we understand your issues and challenges and have in place audit and assurance solutions to manage your risks so as to reduce the impact they could have on you, your stakeholders, and most importantly your students and service users.

Additionally, we have provided a view of the key emerging technologies that highlight risks and opportunities for the Education sector and will continue to do so at an accelerated rate in the future.

‘The extent of the Cyber Security threat to institutions is growing in line with the growth in digital information.’

Cyber security and universities report – Universities UK
The Education sector

The diagram below depicts typical IT risks for the Education sector. We have depicted each IT risk as a bubble with the size of the bubbles representative of the magnitude and impact of each IT risk. These risks should be considered as part of Higher Education’s and Universities’ risk management programme for 2020.

Legend:
- Identified key risks
- Further risks
- Emerging Technology risks
- Strategic/ execution/ business change/ risks

*DSP Toolkit is only relevant to Universities who process NHS health data or have a medical school
2020 technology issues for the Education sector

Data Privacy

The Department for Education (DfE) has revised its Education Technology Strategy in April 2019. Data Privacy has been considered a key risk to be addressed in order to meet the aims of the strategy, and the protection of student data has been highlighted as a priority.

The criticality of information across all industries including Education providers has never been greater, with strategic decision-making often based directly on the results of data analysis, and the repercussions for the data’s misuse at an all-time high.

This is partnered with the fact that advances in technology are now reliant upon data more than ever, and the ethics of such use draws a fine line between innovation and misuse.

How can we help?

Organisations within the education sector hold personal and sensitive data that can range from a student’s name, to serious safeguarding issues affecting children. We can offer a number of services tailored to your privacy maturity, to ultimately improve your data privacy control framework.

Universities using NHS patient data are also required to submit a Data Security and Protection toolkit self-assessment. We have worked with clients to perform a gap analysis in this assessment and provide an independent review.

Cloud Implementation

The DfE’s strategy highlights that Cloud based storage solutions are more secure, cheaper to run, and enable a more robust approach to IT infrastructure. However, cloud adoption does create a new risk in itself.

Firstly, cloud implementation programmes are complex and can require projects within the programme to be delivered simultaneously by different teams. This can often result in logistic and scheduling issues causing disruption and additional work during the build phase for Cloud Implementation Programmes.

Secondly, the adoption of cloud does not transfer risk to the third party cloud provider; new risks need to be considered. Has the correct third party due diligence taken place?

Cyber

The National Cyber Security Centre has identified Phishing, Ransomware, and culture and awareness, as three of the biggest risks to Higher Education (HE) Providers with regards to Cyber Security.

These risks are extended by the resourcing restraints for Cyber Security across the sector. The digital service provider for academia, Jisc, identified that only 60% of HE providers have a strategic Cyber Security Lead.

Across the sector, the sensitivity and value of research data and vulnerabilities of legacy systems increases the importance of cyber security, and the need to ensure controls are in place to safeguard the organisation against cyber threats.

How can we help?

We can provide a number of Cyber assessments based on your maturity and cyber risk appetite. This can include assessment against national and international standards, including: Network and Information Systems Directive (NIS), Cyber Essentials, and the Ten Steps to Cyber.

Further, we can provide a Cyber Maturity Assessment against our own framework, that can provide a maturity level based on global cyber standards.

IT Infrastructure

Aging IT Infrastructure can impede IT advances, and this was noted as one of the biggest barriers to achieving the EdTech strategy by the DfE.

Advanced tools and machines, like cloud or virtualization function very differently to legacy tools and machines therefore issues are likely to arise such as ensuring staff acquire specific experience.

Replacing legacy systems with more advanced ones enables Education providers to become more advanced and offer a better teacher and student experience.

Legacy systems can also increase the risk of technical debt. Without constant incremental changes to systems, there is a risk they will become unfit for purpose, and require additional investment in time and resources to rectify shortcomings.

How can we help?

A lack of IT infrastructure is one of the biggest risks to the delivery of the DfE’s EdTech Strategy. We can provide a diagnostic service to our clients to help identify IT Infrastructure weaknesses, and provide recommendations on how this can be improved to meet the DfE target operating model. We can support you through every stage of the IT change journey, from the hardware of the estate to the skills and capability of the workforce.
## 2020 technology issues for the Education sector

### Budget Restraints

With the proposed fee changes reducing the cost of an undergraduate degree from £9,000, to £7,500 per annum, the possible ramifications are likely to be widespread across all departments within Higher Education Providers. With IT investment and resourcing already limited for Education providers, the potential additional budget cuts could further limit the ability of IT departments to meet overall the demands of the organisations strategy.

### Service Desk

Service Desk is considered to be the central point of contact between service providers and users on a day-to-day basis. Due to the siloed nature of Higher Education providers a centralised service desk is key for monitoring and resolving incidents, disruptions and requests.

Without an effective and centralised Service Desk function there is a risk that incidents will not be escalated and resolved in an appropriate manner.

### De-centralised IT

IT applications existing outside of IT control frameworks may not be visible to Central IT, and may therefore be creating risk that has not been measured and may not be adequately mitigated.

De-centralised IT is growing at pace as organisations strive to be more agile, flexible and competitive, providing faculties with a level of autonomy. This creates security risks as these applications can’t be secured in the same way that supported, authorised apps are secured. There is the added consideration of Research data which has significant value in universities and may be of interest to 3rd parties.

### Data Governance

Universities can amass significant data stores, much of this is personally identifiable, commercially sensitive or has significant value (i.e. research data). It is crucial, therefore, that this is managed and governed effectively to ensure that ownership and accountability is clear and integrity is maintained.

Having an established and effective data governance structure is a common failing. We see the contributing factors being the complex organisational structures and devolved nature in which they tend to operate.

### Legacy IT

Aging legacy systems can impede IT and teaching advances. Legacy IT infrastructure or applications are prone to instability due to failing components, and risk disrupting the overall service.

Advanced tools and machines, like cloud or virtualisation, function very differently to legacy tools and machines therefore issues are likely to arise such as ensuring staff acquire specific experience. Replacing legacy systems with more advanced ones enables organisations to become more advanced and offer a better academic experience.

---

**How can we help?**

We can provide a diagnostic review of your IT Strategy, and provide an assessment on resourcing, priorities, and capability to deliver said strategy.

With the growing reliance on technology we can evaluate the adequacy and effectiveness of the ICT Service Desk, including reviewing the governance arrangements and supporting policy documentation, processes for handling incidents and service requests which impact business users.

We provide a Shadow IT assurance program which seeks to:

- Provide management with an assessment of shadow IT policies, procedures and operating effectiveness;
- Identify control weaknesses that could result in proliferation of shadow IT solutions and greater likelihood that shadow IT is not detected.

We have a team of specialist data governance SMEs within KPMG. We will provide a view on just how clear and well defined the governance of data is within the University. We will then test this view by examining critical data sets and confirming accountability, integrity, availability and completeness. We will also map the data feeds to provide a view on duplication or supplementary data records.

Aging legacy systems can impede IT and teaching advances. Legacy IT infrastructure or applications are prone to instability due to failing components, and risk disrupting the overall service.

Advanced tools and machines, like cloud or virtualisation function very differently to legacy tools and machines therefore issues are likely to arise such as ensuring staff acquire specific experience.
Emerging technology issues for the Education sector

**Artificial Intelligence**

Key issues arising from the use of AI include: gaps in corporate governance and whether AI is operating in line with ethics and values; algorithm bias; re-registration/validation of algorithms; data quality; making data exportable and interoperable and regulatory constraints.

Additionally, building public trust is fundamental as the public need to want to share their data with third parties for AI to harness its potential.

How can we help?

KPMG has developed an AI Control Management framework covering 17 categories for managing risks and controls for AI solutions. More specifically, this has been tailored to AI solutions (i.e. solutions that include machine learning capabilities). KPMG can use its AI in control method to provide guidance and ensure that Higher Education is ready if they have not yet implemented AI and assurance around current processes for the sector with AI implemented.

**Automation**

Education faces IT risks through the adoption of new emerging technology. One example is through the use of robotics for automation of campus management and services.

With technology rapidly changing and an increasing use of automation, robotics, and Internet of Things (IoT), being used to enhance student experience, develop research, automate processes, the Education sector must carefully consider the new rules and regulatory requirements set forth and risks involved.

**Blockchain**

Our clients in the UK are increasingly looking to digitise records and transition to a paperless future; an increasing number of Universities have introduced this with demonstrable benefits.

As Blockchain technology matures the shift to digital records will accelerate. Additionally, through tokenisation of various asset classes, security within Higher Education can be improved.

How can we help?

Despite the benefits to using distributed ledger technologies (such as Blockchain) to store data, as per any digital process, a new set of risks need to be understood and controlled. In order to give assurance to our clients who are adopting distributed ledger technologies, we have developed a Blockchain Maturity Model that assesses the Blockchain maturity across eight key risk areas. We are able to provide an overall maturity score, and specific recommendations targeted towards the key risks.

**DevOps**

As DevOps grows increasingly attractive for Universities, it is important to consider how you can benefit from their use and the risks involved.

Developers/third party suppliers are being used to transform Higher Education IT infrastructure through use of agile methodology. This may include implementing changes directly into the live environment thus, posing challenges and risks to the adequacy of changes, data integrity or customer satisfaction.

How can we help?

KPMG offers DevOps based solutions from preparing thorough assessment and analysis reports, helping to integrate tools and administration to delivering professional services and training.

We can assist in the alignment of your DevOps, IT, and business teams to build successful Higher Education reaping the business benefits available from DevOps.
KPMG has an experienced team of Technology Risk Consultants that are constantly working with our clients to develop their approach to IT Risks.

Our aim is to help you identify, optimize and manage your risks in this area in a cost effective way. To discuss please contact:

**Nicolina Demain**  
Technology Risk Director  
Higher Education Lead (Tech Risk)  
M: +44 (0)7748 885220  
E: nicolina.demain@kpmg.co.uk

**Tim Colclough**  
Technology Risk Manager  
M: +44 (0)7887 826733  
E: tim.colclough@kpmg.co.uk

**Lee Dobbing**  
Technology Risk Senior Manager  
Higher Education SM (Tech Risk)  
M: +44 (0) 7919 293691  
E: lee.dobbing@kpmg.co.uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.