

# Risk management in digital transformation for universities

19 April 2021

In the past year, the pandemic has accelerated digital transformation in the higher education sector, with the majority now anticipating that a hybrid learning model blending digital and in-person teaching methods remain the norm.

This will require far more than simply translating traditionally delivered material to on-demand media. To remain competitive universities must embed the digital experience into their curricula from the ground up. Students in 2021 expect seamless integration of the systems they use for learning, to facilitate an increasingly personalised service delivery which meets their individual needs and preferences. While this new digital environment brings many advantages, there are also challenges for IT departments in integrating new technology.

## Design and planning

The role of technology in higher education is now front and centre on the agenda, but the success of digital transformation programmes in the sector requires engagement from stakeholders across departments, who can offer valuable insights into the needs of future students. The landscape is shifting so rapidly that designing a digital strategy purely around the way the university currently operates is likely to render it outdated almost before it is implemented. Successful digital transformation projects will require universities to procure new software and platforms in alignment with current needs, whilst also allowing for development over time as students' learning habits, living patterns, and expectations change.

## Practice points

**Contract governance** is key. Once an IT solution has been procured, all too often its implementation and support are managed without reference, or with only minimal reference, to the contract itself. However, the contract is central to managing risk, and often includes helpful provisions enabling a dissatisfied customer to exert pressure on the supplier, which can assist in renegotiating terms where that is desired. Where changes to the contractual scope are required, it is important to document them using the contractual mechanism for doing so, in order to record agreement as to whether the supplier or the customer is liable for any concomitant increase in costs, and as to the impact of the changes on the contractual timescale.

**Third party IP rights must be kept under review.** Higher Education Institutions need to monitor how they are licensing software to ensure that the arrangements they have in place adequately match the ways in which students and other users are accessing their systems, particularly as student living and working patterns become more flexible in the future. Issues can arise where, for example, there are geographical restrictions on where software can be accessed, and students' locations cannot be as accurately predicted as was the case prior to COVID-19.

**Data security.** Universities hold a vast amount of personal data relating to students and staff, as well as valuable data generated through research. As such, they are attractive targets for cyber-attacks. In addition, there are many more routes into a university's network than is the case for most large companies, by virtue of the number of students connecting personal devices to the university network. It is almost impossible to protect fully against a cyber-attack and so having robust and defensible processes in place to deal with one when it occurs is essential. This should include GDPR and IT security training for all staff, as well as having technical and organisational measures in place to ensure (as far as possible) that cyber attackers will not be able to access systems, and disaster recovery and business continuity

plans to implement in the event of a major incident, as these factors are taken into account by the ICO when setting the level of any fine following a data breach.

**Systems integration.** Traditional departmental structures make decentralised IT systems a common feature in many universities. The result can be a web of disparate infrastructure which can hinder the adoption of new technologies due to the difficulty and cost of integrating legacy systems with new systems. Where new systems are procured, a thorough analysis of the need giving rise to the procurement, and level of customisation of the new solution required in order to integrate it with existing systems should be conducted in conjunction with the supplier, to mitigate the risk of expensive changes to project scope, and arguments about who should pay, later on.

The focus should always be on avoiding disputes with suppliers in the first place. In many cases this can be achieved through more active contract management, and through building sufficient flexibility into new contractual arrangements to be able to adapt to the rapidly changing landscape of student needs. Where difficulties or disputes do arise, early analysis of the parties' contractual obligations against what has happened is paramount, to avoid inadvertently waiving any valuable contractual or common law rights and to ensure that all available legal mechanisms can be deployed to best advantage to manage risk and resolve the issue.

For further information and support on any of the above issues, please contact us.

## Contact



**Mark Hickson**

Head of Business Development

[onlineteaminbox@brownejacobson.com](mailto:onlineteaminbox@brownejacobson.com)

+44 (0)370 270 6000

---

## Related expertise

### Services

Research, knowledge transfer  
and digital innovation in higher  
education