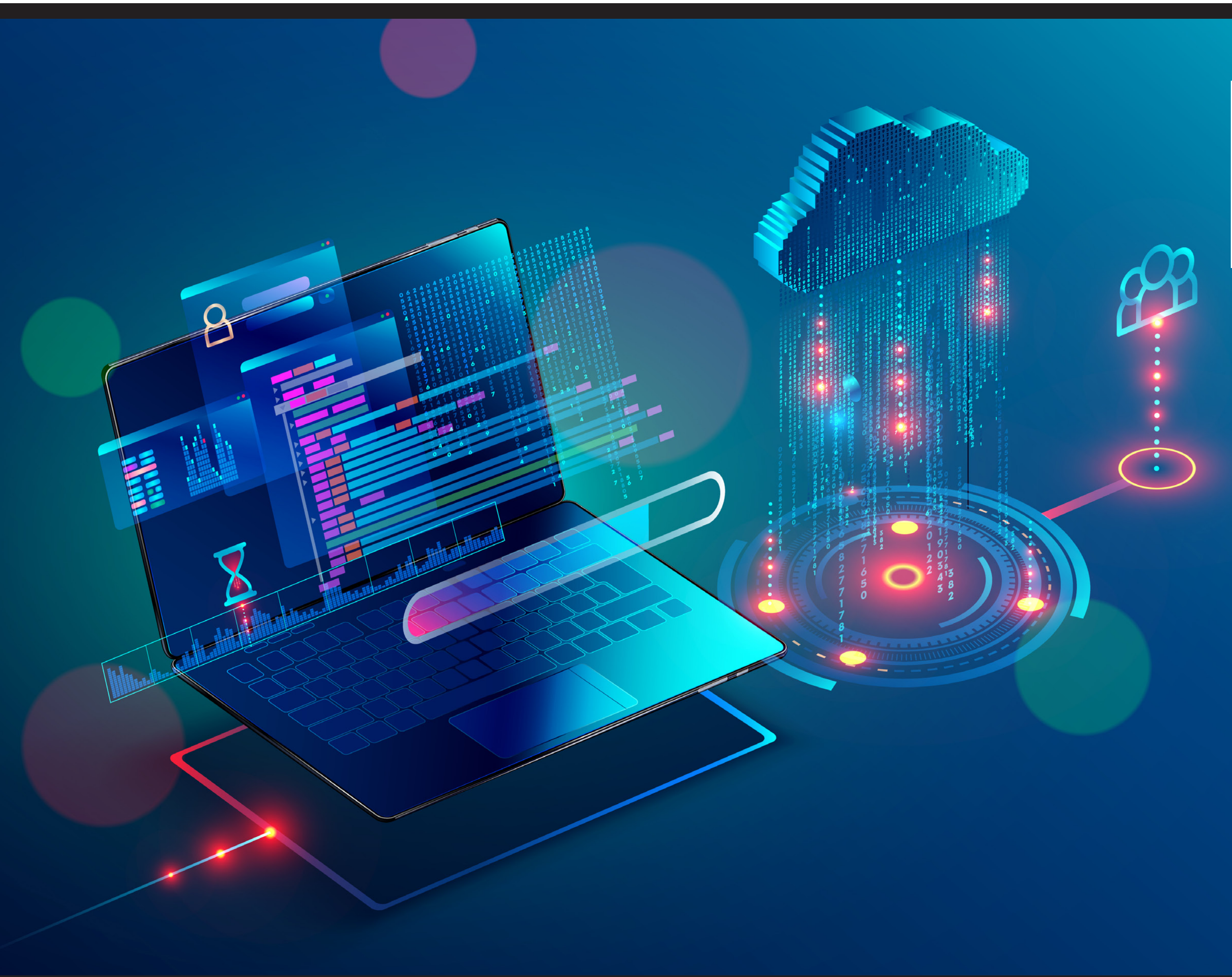
FStech

Sponsored by:

Creative ITC

NetApp
Gold Partner



Roundtable Special

Creative ITC

Rethinking the Risk of IT Outsourcing

FStech and Creative ITC brought together a group of senior IT executives from across the financial services sector to discuss the most pressing issues in emerging trends in moving technology to third parties.

Keeping IT in-house can cause staffing headaches and drain investment from other areas, but outsourcing has its own set of risks – from regulatory responsibility to data security oversight and maintenance of on-site systems.

Increasingly though, to keep pace with digitally-native challengers, using third party providers for IT infrastructure and cloud-based platforms is crucial to gain and retain customers and clients.

This roundtable examined the various due diligence questions businesses should ask, debated the pros and cons of different strategies being used, and assessed the threats posed by political upheaval, cyber criminals and compliance.

Paul Shambrook, solutions architect at Creative ITC, kicked things off by explaining that he has found client IT budgets are increasingly stretched, so staff cannot afford to look after every single thing in their estate. This encouraged the company's move into managed services, as demand grew for management and monitoring, on top of the original technology build.

Others in the room shared their reasons for attending, with several citing problems with handing off IT estate to third parties.

Time, money and reputation

One participant who worked for a bank commented that regulators now expect several levels of due diligence to have been undertaken during any outsourcing decision.

"We all do our due diligence on our suppliers, but how far do they expect us to go? With that last paper on operational resilience last year, which was the first joint paper from the FCA I can remember for a while, it's a really hot topic," they stated.

As well as the clear regulatory risk, TSB's botched IT migration last year was cited as a case of the reputational risk of getting these things wrong.

"It's management time, because their PRA will be crawling all over them for a very long time, that will cost them a fortune in consultancy, lawyers and just not being able to do anything else," they added.

Another person round the table told of how they had recently moved on from a bank where the onboarding process could take up to nine months, which seemed to be "risk management gone too far".

At their new employer, things were quicker as the organisation is smaller, but there were still forms to fill out in order to get some staples. "I want to know not just how we can manage risk of outsourcing, but how we make it a competitive advantage, how can we make it more efficient so I don't have to write out a form to get some staples."

David Gould, director of digital delivery and architecture at Metro Bank, explained that his company was one of the founding members of the Financial Services Supplier Qualification System (FSQS), which puts third party suppliers through a risk assessment to give firms a list of pre-approved options when outsourcing.

"We basically ask them 10 questions and based on those they understand the risk profile as best we can – if you're a supplier coming into the banking sector, you only do it once and you automatically cleared to work with lots of banks," he stated.

Of course, depending on the answers to those first 10 questions, more may be asked, with vendors ranked into tiers depending on accountability and other factors.

"The suppliers hate it, there's no doubt, particularly a lot of the smaller ones, if you want to work with some of the more FinTech, boutique startups, they're just not geared up for that, they don't have the resources for it," added Luis Aguiar, head of digital engineering at Metro Bank.

"But for a FinTech, once you're on the list you can go and knock on doors and say hey, I'm on the list, which opens up much easier conversations with big banks."

One person commented that every different client they worked for had a different approach to auditing, with no standardisation possible to speed up the process.

"We tried the approach of 'these are the main things that we get asked all the time', but it was never good enough, the audit team would always need to come in and we would spend an inordinate amount of time dealing with the security teams and risk teams, where they really wanted to go to a very deep level to satisfy themselves of what we were telling them was true," they stated.

It really was a heavy workload across the organisation and cost a lot of money, because everybody we dealt with - maybe because of their size, some were small, some were quite large - they all wanted to come and audit us once, twice a year, so it was almost a full-time job just responding to those audits," they continued, adding: "Very often some would be paper-based, very often they were onsite-based, we'd have relationship managers hosting those guys for two or three weeks."

Another participant pointed to the American system of a standardised questionnaire of typical questions, or even better an annual self-assessment system, but someone else argued that bosses would rather get an external audit than have to rely on internal teams to carry out the work.

The biggest barriers

Moving on to other barriers facing financial services firms looking to outsource, one attendee admitted that the previously stated nine months seemed almost agile compared to some of the project constraints he had faced due to government frameworks and procurement rules.

"I think the problem is that we have to go through certifications for every element of a project, which can mean that if a services provider doesn't quite fit the mould then it's 'computer says no' and we have to reject them," they stated. "To keep on top of that framework, it would be a whole team of people with a huge overhead, which just isn't worth the investment."

Someone else pointed to openness from potential suppliers as another challenge. "Typically you might get responses of 'we're not giving you that information' for competition and confidentiality reasons," they noted.

Another complained that many times it comes down to suppliers pointing to their relevant ISO certificate, which can begin to be a false sense of security and "not worth the paper it's printed on".

"It's always a tricky thing to design a certification that doesn't become jumping through hoops," one participant added.

Maxim Gente, an executive director at Credit Agricole, said that another problem is resource attrition, as his company cannot directly incentivise people who work for the vendor.

"So for example, I have a valuable resource that I would like to retain, I can't really do anything about his or her salary; it's up to the vendor to do it. If they don't, then that resource will leave, which will expose me – this is what I have to deal with on a monthly basis."

In-house or India?

Taken as shorthand for third party providers in countries where skilled labour is cheaper, the conversation turned to the relative value of outsourcing IT to India, with several participants questioning the initial rush to do so.

"It's much easier to manage captive than to manage a vendor - the vendor has a different set of incentives and they have their own bottom line and all that kind of stuff - if you have some reliance on resources which are provided by the vendor, you are sometimes simply powerless to fight attrition," stated one person round the table.

While going 'captive' is certainly more expensive on paper, in practice it is often much easier to manage relationships and resources under one roof, especially given cultural and conduct differences between countries.

Another person round the table said they would not only outsource to 'nearshore' suppliers. "One of our relationships the back office was in Boston and it was a daily operations thing. Of course there were people in at 5am in the morning, but they're always junior, so if you had a problem, you could never get anywhere until lunchtime.

"Interestingly enough, they actually moved most of their back office from Boston to Poland and the service improved immensely from our point of view, because now they're on the same time zone as us."

Money talks

Looking at the other side of the relationship, talk turned to the leverage that can be gained by being a vendor's biggest client in terms of IT spend.

"There is this sort of cycle of the engagement of the vendor," explained on partcipant. "What happens is when they want to get you in the door, the best guys are going to show you everything, give you some resources for free, as long as they get the account.

"You'll have a honeymoon period, but as soon as they've got their feet under the desk and they start getting comfortable, the best people move on to win new business," they continued, adding: "Until there's a problem, then they bring their best guy back in and he says I'll sort it for you, don't worry."

Paul Shambrook interjected to say that Creative ITC take a lot of business from multi-department organisations like BT, "because we're not trying to take their whole environment or the whole infrastructure; we're outsourcing an element where we're a specialist; we're not trying to boil the ocean".

He continued that these bigger businesses will often work with several specialist suppliers, rather than have all their eggs in one basket with one supplier across the tech stack. "I appreciate there's an overhead on you guys to maybe manage three suppliers instead of one, but it keeps us invested, it makes sure that we do have good people on site, that we can't just chop and change people."

External issues

To conclude the evening, the debate moved onto how changes to the political, regulatory and security landscapes are impacting IT digitisation programmes.

"We're seeing a huge increase in questions about cyber security from clients, I think it's become apparent to people that in terms of managing the risk penetration within their own systems, anyone who's doing their job well has probably got a good idea where their risks are and how they're mitigating them," commented one participant. "It's becoming apparent that the third party suppliers are often back door in, so we're certainly seeing quite a large increase in people saying 'we've got connections to you guys, you've got data on us, what are you doing to keep that safe?' – I can say for sure five years ago nobody asked that."

James Arden, third party security lead at Brewin Dolphin, explained how his previous experience managing security incidents has highlighted the importance of being clear with communications, both internally and externally is incredibly important during a data breach. Notably the differences between the handling of an internal breach, versus those concerning data held by a third party, as they require very different approaches.

Another person around the table said that for vendors, he demanded specific plans for what would be done in such situations. "I've had experience where companies go into every detail about the incident and keep you up-to-date – and that will panic a lot of people."

Someone else responded: "It's a counterintuitive thing though, as if you have a trust-based relationship with your vendor, then they're going to say that, but if they feel they're on a rocky road with you already, commercials can take over and they're going to keep quiet."

Conclusion

Outsourcing has evolved a huge amount since its mainstream implementation in the 1990s, with many lessons learned and solutions developed. The solution presents unique challenges depending on the nature of the service to be provided, and this roundtable established that while there are some initiatives to make outsourced vendor due diligence more standardised and less resource intensive, there is still progress to be made.

Vendors should be chosen according to clearly understood business objectives, agreed by the relevant stakeholders, in order to ensure a balanced approach to selection. Whilst cost is always a major factor in outsourcing decisions, consideration should also be given to what realistic expectation of quality levels is possible when vendors from the lower end of the cost spectrum are selected.