SOURCING IN THE DIGITAL AGE
SHAPED BY DISRUPTION

Nick Pantlin, Jeremy Purton, Alex Cravero and Claire Wiseman of Herbert Smith Freehills LLP discuss how new disruptive technologies are shaping current sourcing strategies.

Many people believe that we are currently witnessing a fourth industrial or technological revolution, with the advent and increasing use of a wave of disruptive technology. Over the past five years, the market has seen the arrival of a range of new technologies that have transformed the sourcing market and delivery models for both IT and business process service offerings. These include: multi-tenanted platform provision, such as cloud-based services; robotic process automation (RPA); machine learning; artificial intelligence (AI); the internet of things; blockchain and distributed ledger technology (DLT); and smart contracts.

Increasingly, organisations are having to think like technology companies as they look to explore and assess the opportunities, as well as the commercial and legal risks, presented by these technologies and alternative delivery models.

As a result, conversations around technology-driven transformation and sourcing strategies are now board-level agenda items. These conversations are closely aligned with two other critical executive concerns: data protection and data use following the recent entry into force on 25 May 2018 of the General Data Protection Regulation (*679/2016/EU*); and cyber security risk with the entry into force on 10 May 2018 of the Network and Information Security Directive (*2016/1148/EU*) (NIS Directive) (also known as the Cybersecurity Directive).

This article considers:

- The challenges and opportunities presented by new technologies from a sourcing perspective.

- The key trends and drivers behind recent changes to sourcing models.

- How businesses engaged in sourcing (both customers and suppliers) could deploy more effective sourcing strategies to keep abreast of technological change as disruption continues to be a key feature of the digital economy.

THE CHALLENGE OF DISRUPTION

The days of a sourcing strategy being just about reducing cost are gone. While cost drivers are still important, discussions regarding sourcing strategies now increasingly take place at senior management level as the highest-level executives want to understand how they can use digitisation and technology to:

- Enable transformation.

- Exploit and protect their data, which, for most organisations, has now become their most valuable asset.

- Drive revenue growth as part of business change.

For incumbent companies across all sectors (including financial services, energy, transport, consumer, retail and healthcare) which have not traditionally had to think like technology companies, this has led to an increased need for guidance from their advisers on assessing the benefits, challenges and risks of incorporating disruptive technologies into their supply chains and how doing so may contribute to long-term success.

As supply chains become increasingly complex and disaggregated, there is also a need for organisations to address the difficult challenge of deciding which functions and roles should be retained and further developed in-house, as being core or strategic to the business, and which ones should be outsourced to third-party specialists.

If incumbent companies do not embrace the digital age as they develop and implement their sourcing strategies by, at the very least, becoming fast followers of technology, they risk being left behind or losing market share to those who are prepared to invest in and embrace change, and better adapt their business models for the digital economy.

The importance of data
The advent and growth of new technologies all have one vital ingredient at their core: data.

Data have been described by some as the fuel of this fourth industrial revolution or the technology age. According to a recent IBM report, 90% of the world's data collected to date has been collected in the last two years and daily data generation is exponential as virtually every activity creates a digital trace (*available at www.ibm.com/ account/reg/us-en/signup?formid=urx-13776&LeadSource=MC_Q4-16_2017Trends_ MP_Hotline_70133000001UE3C&Engage_ Campaign_Status=Registered&Promo Code=MC_Q4-16_2017Trends_MP_ Hotline_70133000001UE3C&Engage_ Campaign_ID=70133000001UE3C*). Big data is just getting bigger. This explosion of data has come about because of the enormous increase in computer processing power, one product of which is the cloud infrastructure and vast data centres being built by the technology giants, which are the engine rooms of the cloud.

GDPR and NIS Directive

The General Data Protection Regulation (*679/2016/EU*) (GDPR) came into force on 25 May 2018 (*see News brief "EU General Data Protection Regulation: on your marks, get set, go!", www.practicallaw.com/w-014-9290*). It introduced some key changes that are now giving rise to closer scrutiny of the supply chain protections in place between controllers and processors, for example:

- Processors now have direct statutory obligations and liabilities for the first time in certain areas.

- Controllers are now required to impose specified mandatory data processing provisions on processors under Article 28 of the GDPR, including provisions around the process for appointing sub-processors and the flow of obligations to those sub-processors, and audit requirements. These may give rise to challenges when transposed to complex supply chains such as those involving multi-tenanted platform service providers.

- The increased sanction regime under the GDPR carries monetary penalties of up to a maximum of 4% of annual worldwide turnover or €20 million, whichever is the greater, for certain breaches.

This shift in risk profile for both controllers and processors gives rise to a very different risk assessment for those parties. In addition, the liability regime for breach of data protection provisions has been elevated in importance, in particular with the need for clear contractual allocation of responsibility and liability for data protection between those parties, and any sub-processors. It is equally important to balance this risk allocation with the need for a co-operative relationship between the controller and processor (for example, if there is a cyber incident) to best resolve any potential issues in the quickest and most effective manner.

The GDPR also enshrines concepts such as data protection impact assessments, and privacy and security by design, requiring controllers to think about privacy and cyber security at the inception of projects and systems. As a result, more organisations are seeking early engagement with potential suppliers, and data protection and cyber security requirements are being addressed as key criteria in a request for proposal.

From a cyber security perspective, customers and suppliers also need to take account of the implementation of the Network Information Security Directive (*2016/1148/EU*), which entered into force on 10 May 2018, and applies to operators of essential services and digital service providers (*www.practicallaw.com/w-014-9609*).

With increased outsourcing to the cloud or other third-party external service providers, and an increasingly complex supply chain for businesses, modern strategies for leveraging data can bring significant business efficiencies, competitive edge and growth opportunities. There has been a growing awareness by organisations of how using this increased computing power and innovative technology to collect more data about their business and apply it to existing and ever-developing data sets can yield invaluable, and monetizable, insights.

However, while one of the most obvious opportunities that disruptive technologies bring is the application of smart technologies to large data sets, both customers and service providers will need to ensure that their contractual arrangements, and technical and organisational measures, appropriately address issues and challenges relating to the collection, storage, processing and retention of personal data (*see feature article "Data use: protecting a critical resource", www. practicallaw.com/w-012-5424*).

Therefore, businesses need to consider both how to exploit their data for commercial gain and how to keep the data safe and compliant with regulatory requirements (*see box "GDPR and NIS Directive"*).

NEW TECHNOLOGIES

No one should be surprised at how technology applied to a business problem in any sector can result in a comprehensive transformation of how participants in that sector conduct business. The sourcing market is no exception and there is an increasing amount of deal activity where customer organisations are seeking to harness the benefits of new technologies and expecting suppliers to demonstrate how new technologies can improve efficiency and effectiveness.

Many disruptive technologies are beginning to make their presence felt in supply chains, sourcing models and customer-side user requirements (*see box "Effect of new technologies on sourcing practice"*). These include RPA, AI, and blockchain or distributed ledger technology and smart contracts.

RPA

RPA is the automation of high-volume, repetitive and routine tasks using computer software that is capable of complying with codified rules and instructions. RPA is not strictly a new technology as, for many years, programmed automation has been successfully implemented in a number of sectors that are heavily reliant on structured data and standardised processes, such as the automotive sector, to increase productivity and decrease the cost of process-driven tasks. However, until recently, the use of RPA in the context of outsourcing arrangements has been comparatively limited.

Previous decades have seen repetitive and routine tasks that would otherwise have been carried out by costly onshore labour resources outsourced to service providers based in offshore locations such as India and, more recently, repatriated but to lower-cost regional service centres. The lower cost associated with these offshore and nearshore locations translates to a lower cost per full-time equivalent resource (FTE), which in turn provides customers with significant cost savings even where the overall volume of FTEs carrying out tasks can often remain unchanged or be reduced only marginally.

However, outsourcing to offshore and nearshore locations is not without its limitations. In particular, the continued reliance on human resources means that cost savings are necessarily limited to the difference between the on-shore and off-shore cost profile and, as with any task that

involves human actors, there is an inherent risk of error in processing activities. Other environmental and jurisdiction-based external factors also present natural limits to the level of efficiency and cost savings that can be achieved, particularly where offshoring results in higher compliance costs, such as where data processing is transferred outside the EEA.

Benefits of RPA in sourcing. Lower hardware costs, ever-increasing computer power and the growing availability of cheaper, decentralised cloud processing and storage services is making RPA an increasingly affordable and attractive option to customers that wish to outsource high-volume IT support, workflow and back office tasks. These might include creating reports, reviewing and managing emails, inputting into and submitting forms, and operating payroll and book-keeping systems. Many of the big IT service providers are also expanding their service offerings to encompass what would traditionally have been the domain of HR-based business process outsourcers.

RPA is increasingly being used to analyse policies and claims, detect fraud, and for marketing. In addition, RPA can often process large and unstructured data sets more efficiently than human-based services, and better manage the transfer of data between different interfaces, replacing what would otherwise be human application programming interfaces (APIs).

The automated nature of the computer software used in RPA broadly resolves the issues commonly associated with traditional outsourcing by removing or reducing the risk of human error involved in completing repetitive

and routine tasks. The use of programmed, intelligent automation such as RPA means that the number of human resources and total FTE-hours spent carrying out high-volume tasks can be significantly reduced by replacing those low-skilled resources with computer software that is programmed to follow clear rules and instructions.

Issues with RPA in sourcing. While human error is reduced or removed from the performance of the low-skilled task, humans are still responsible for codifying the initial rules and instructions that are to be followed by the computer software. The automated output of the computer software therefore remains susceptible to human error in the codification of the rules and instructions.

AI

AI encompasses computer systems which can perform tasks that usually require human intelligence, such as visual perception, speech recognition and decision-making. While in its relative infancy, AI is already generating a significant amount of hype in the outsourcing industry.

AI shares some similarities with RPA in that it is a form of intelligent automation. However, unlike RPA, which is a programmed, trigger-based automation, AI's use of cognitive decision-making processes means that it is more autonomous and capable of self-learning, and therefore potentially capable of replacing a range of "higher order" activities that would otherwise remain the preserve of human actors. AI programs can be trained, or can train themselves, to automate complex and subjective work through pattern recognition, to process natural language

and unstructured data, and to respond to changes, without further human input or direction.

While service providers often refer to AI as being currently available in the market, these references are generally to "weak" or "narrow" AI; that is, AI which is able to develop human-level or greater cognitive ability with respect to a single defined task, like beating a human at chess. The development of "strong" or "true" AI; that is, AI which is able to develop human-level or greater cognitive ability across multiple tasks, remains immature. Many broadly consider that the forthcoming decades will see this technology perfected and become widely available for commercial use.

Benefits of AI in sourcing. Much like RPA, the automated nature of AI software will address many of the risks and issues that are currently experienced when customers outsource processes to offshore service providers. In particular, the cost savings available to customers should increase and the risk of human error should decrease. This reduction in human error also has the potential to positively affect service performance, for example against service levels, which, in time, may need to be recalibrated.

As AI technology improves and businesses' access to computing power and storage increases, AI has the potential to be genuinely transformative in the handling of business processes and in the application of AI learning to large, unstructured data sets.

Issues with AI in sourcing. Inevitably, AI is heavily reliant on the data that is given to it. The relevant tools need to be able to identify the limits of their own capability and call on human intervention when needed. There must also be absolute assurance of the privacy, accuracy and completeness of the data being processed by the tools and of the output that the solution delivers.

As well as the importance of reliable data sets, the smart algorithms behind AI solutions need to be integrated with legacy systems and to support the end-to-end processes that humans still need to do.

In addition, customers will also need to consider the risk allocation between the parties in terms of the decisions made by the AI. Current contractual methods of apportioning liability between parties will

inevitably undergo change as the market begins to react to the implementation of AI, and it is likely that there will be a number of challenging disputes that will play out as the market and legal position settles.

DLT and smart contracts

DLT is where a decentralised ledger of transactions can be maintained collectively by its participants, rather than by a trusted third party, and amended only according to strict rules and majority consensus. DLT has given rise to new technologies capable of benefiting both customers and suppliers in the outsourcing industry (*see Briefing "Blockchain technology: emerging from the shadows", www. practicallaw.com/4-634-8506*).

One of these technologies, which can be built into a DLT network such as blockchain (but which is not exclusive to DLT networks), is smart contracts; that is, computer code that reflects a business arrangement and can automatically self-execute on the occurrence of certain pre-defined conditions.

The term "smart contract" is, from a lawyer's perspective, something of a misnomer. Smart contracts are not contracts in the legal sense; rather, they are perhaps better described as "if then" and "if-then-else" statements comprising computer code that is designed to self-execute, and which may do so on a distributed ledger or any other network or platform. However, when applied to a legally enforceable agreement, therefore forming a "smart legal contract", the self-executing computer code is capable of verifying, facilitating, monitoring and enforcing the performance of the agreement without the need for human intervention.

Benefits of DLT in sourcing. The automated and deterministic nature of smart legal contracts means that they are able to reduce or remove the risk of human error in managing contractual performance and enable parties to contract based on sophisticated and novel mechanisms that would be too complex for humans to practically administer. This could be a particularly useful tool in complex multi-seller outsourcing arrangements.

For example, DLT and smart legal contracts could be used in service level mechanisms by automatically managing and controlling adherence to a contractual service level regime. If a supplier failed to meet a service level in a given measurement period, and the failure meets pre-defined conditions such as

a service credit threshold, the smart legal contract code could automatically trigger certain outputs. This may include notifying the parties of the relevant failure or triggering the payment of service credits.

Another example of where DLT and smart contracts could be used is in reporting regimes by automating complex reporting regimes across an outsourcing ecosystem. Reports could be sent automatically to certain participants on a DLT network in the event that specified inputs, such as performance or other metrics, are triggered. If the DLT environment is private and permissioned, these reports would be available only to authorised participants and would therefore be more secure than conventional information storage systems.

Issues with DLT in sourcing. The deterministic nature of DLT networks means that there is a risk that inputs from non-deterministic external data sources, such as service level measurements or reporting triggers, will affect the immutability of DLT or otherwise limit the usefulness of smart contract code, which may be unable to respond correctly to the sort of variation and nuance that are often negotiated into complex services agreements. To resolve this, the non-deterministic external data sources would typically need to be inputted by humans, thereby reintroducing the risk of human error in managing contractual performance through smart legal contracts.

While there is still a way to go, promising progress is being made to resolve these issues. An increasing number of external data sources are now able to be input by "oracle" functions that can be built into DLT systems and which can translate non-deterministic functions capable of change over time (for example, APIs providing service level measurements) without affecting the DLT's immutability.

CHANGES IN SOURCING MODELS

Changes in sourcing practice indicate an evolutionary rather than revolutionary approach to sourcing (*see feature article "21st century sourcing: revolution or evolution?", www.practicallaw.com/2-522-0133*). In addition, customers have had to upskill their own in-house capabilities to get the best out of their sourcing supply chains, in particular to harness the benefits of new technologies, which may be termed the intelligent customer

function (ICF) (*see "Managing integration risk" below*) (*see feature article "Sourcing 3.0: the rise of the intelligent customer?", www. practicallaw.com/1-608-7044*).

Sourcing strategies over the years have been quite cyclical across and between organisations and different sectors. The traditional sourcing models have ranged from in-house solutions, to so-called "big-bang" single sourcing, through to more evolved and sophisticated multi-sourcing or multi-vendor models.
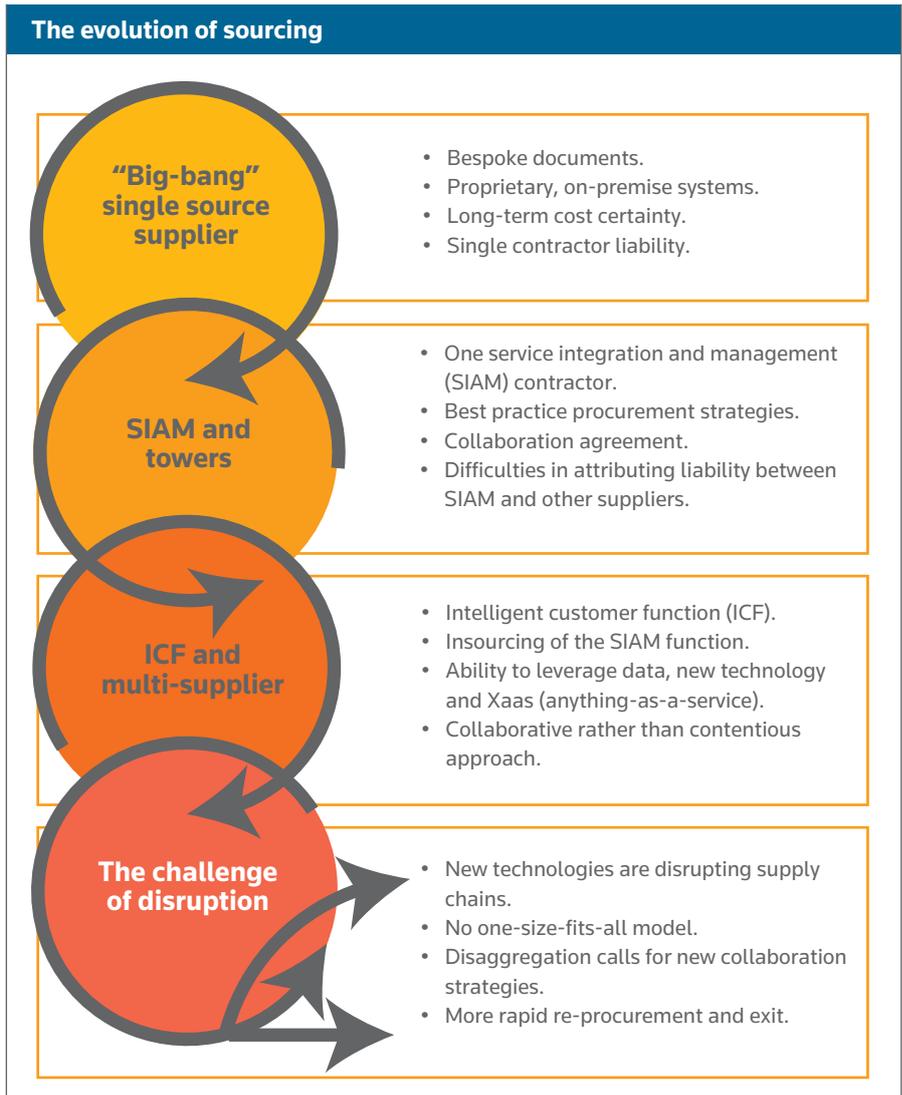
From big bang to disaggregation

With the ever-increasing growth and proliferation of new technologies and delivery models, supply chains are becoming even more complex and disaggregated. Some commentators have described how the global technology industry is experiencing a seismic change as the outsourcing trend of the last decade goes into reverse. It is certainly true that there has been a significant shift from the days of the big-bang, large-scale, single-source deals, when it was possible, or even best practice, for an organisation to outsource the entirety of its IT requirements to one of the traditional IT giants in a long-term, high-value deal.

According to consultants ISG Inc, in 2008, 42% of the largest global businesses outsourced their IT to a single service provider, but that percentage has now dropped to 15% (*www.raconteur.net/future-outsourcing-2018*). The traditional single-source model is being disrupted as customers are moving away from a business case that used to be based on the cost savings derived from the economies of scale of using a single provider for a long-term (typically five to ten-year) contract.

A combination of new technologies, such as the huge growth in cloud infrastructure, software-as-a-service models and RPA, together with increased competition and more sophisticated customers, has shaped an evolution towards a more varied, disaggregated, sourcing model (*see box "The evolution of sourcing"*).

Managing integration risk

The disaggregated sourcing model poses a number of challenges from both a commercial and legal perspective. While disaggregation gives the customer more flexibility and stimulates competition among its supplier base, it also places increased management and integration risk on the customer. With

The evolution of sourcing

"Big-bang" single source supplier
- Bespoke documents.
- Proprietary, on-premise systems.
- Long-term cost certainty.
- Single contractor liability.

SIAM and towers
- One service integration and management (SIAM) contractor.
- Best practice procurement strategies.
- Collaboration agreement.
- Difficulties in attributing liability between SIAM and other suppliers.

ICF and multi-supplier
- Intelligent customer function (ICF).
- Insourcing of the SIAM function.
- Ability to leverage data, new technology and Xaas (anything-as-a-service).
- Collaborative rather than contentious approach.

The challenge of disruption
- New technologies are disrupting supply chains.
- No one-size-fits-all model.
- Disaggregation calls for new collaboration strategies.
- More rapid re-procurement and exit.

every new piece of technology or new solution that an organisation adds to its supply chain, there comes an incremental data breach risk as its IT systems become more vulnerable to potential cyber or other security threats, as well as system outages that may compromise end-to-end stability.

A key question for customers, particularly those in technology, risk and operations teams, is how they will organise themselves and their suppliers to manage the risks involved in joining together different services across different technology stacks, some of which may be the product of collaborative working among a group of suppliers. For example, a future enterprise transformation plan that depends in part on lower-cost commoditised services will need to be all the more mindful of how end-to-end processes can cross service and contract boundaries.

This new integration risk can be addressed in various ways. Early examples created a new service and introduced a new participant:

the service integration and management (SIAM) contractor. However, the SIAM role has become, in many cases, just another bundle of services that a customer has to procure and then manage. Issues around responsibility for cross-service bundle or "tower" defaults, implementation and exit, and dependency management are still difficult, with the (often lower-value) SIAM contractor unwilling to accept liabilities for failures by other suppliers to perform, the consequences of which may be significant for the customer (*see box "Increasing complexity of collaboration mechanisms"*).

Intelligent customer function. The ICF is one way in which customers have sought to mitigate some of these concerns. The ICF is the capability within the customer's organisation which assists in the procurement of outsourced services. For many customers, this has involved rebuilding their in-house service integration and management capability. In some cases, this has been a case of "back to the future" where formerly-
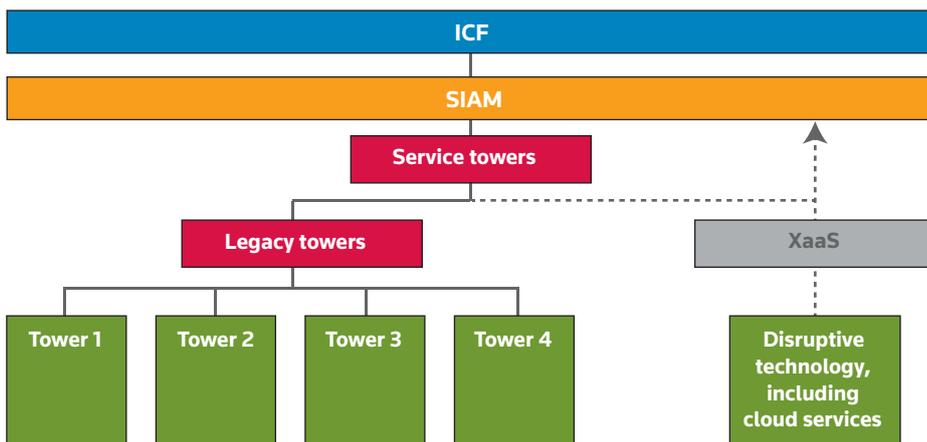
Increasing complexity of collaboration mechanisms

Bilateral or cross-tower collaboration
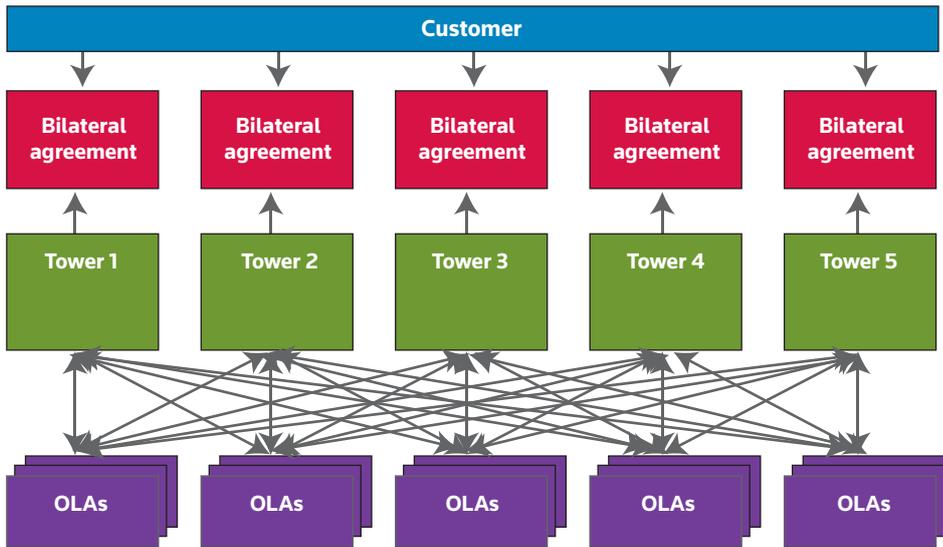
The customer relies on non-binding operating level agreements (OLAs) to ensure interface alignment and operational co-operation between the different service towers.

SIAM and ICF

Both the service integration and management (SIAM) and towers model, and the intelligent customer function (ICF) model, have struggled to cope with the rise of disruptive technology, which leverages cloud and anything-as-a-service (XaaS) models in a way that breaks down service tower-based silos.

Multilateral collaboration
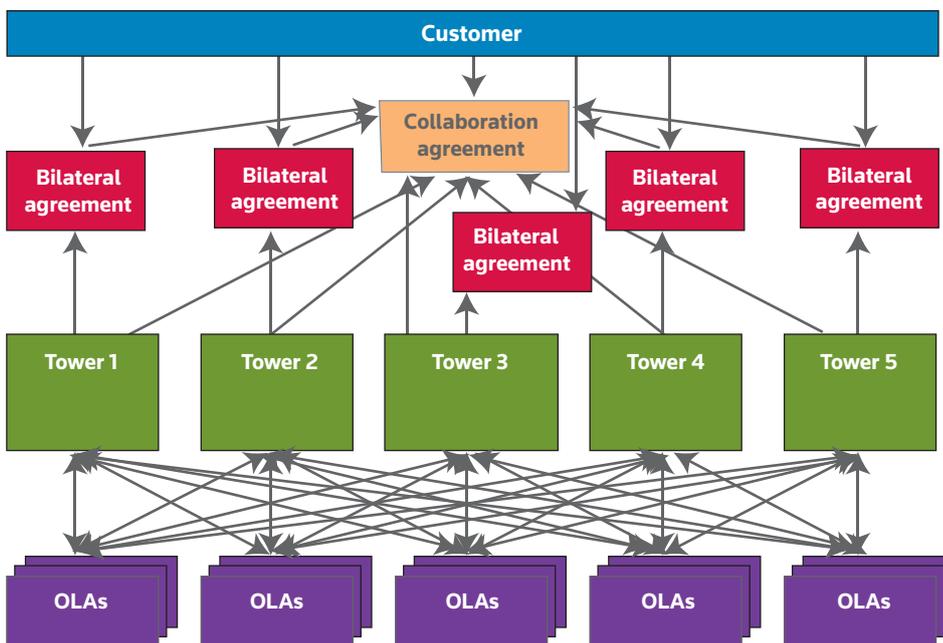
Alternative models that address collaboration problems and manage integration risk have tended to focus on combining traditional approaches, such as OLAs, with more novel, but complex, multilateral collaboration regimes, backed up by binding or non-binding collaboration agreements.

outsourced functions have been brought back in-house as companies realised their strategic importance.

The challenge for customers is investing in, and finding the right expertise to help them run, the ICF. This is why many customers are working with third-party services integration experts to help them build and manage the ICF. The increased complexity of the sourcing and technology solutions available has contributed to this shift from reliance on a few key outsourced service providers to more specialisation and disaggregation. Technology and software has become something that companies cannot simply just outsource anymore. Companies increasingly need to develop their own expertise in-house, with a greater emphasis on collaboration models (*see "Collaboration models" below*).

This means that there is an ever-expanding number of dependencies and procurement obligations on the customer as it seeks to manage the supply chain, particularly as the focus is increasingly around end user-led service design and delivery. While this is nothing new, it has begun to reveal some interesting challenges around the demarcation between supplier obligations and customer dependencies, particularly if the customer is relying on some of its own internal capability to provide key functionality to end users of a service. In this sense the customer has, through its retained service management function, also become a supplier to its own user base.

The ICF has therefore become even more important and should be a key focus for companies going forwards, as they further develop their sourcing strategies to exploit new technologies and delivery models available in the market.

COLLABORATION MODELS

The key challenges for any customer whose sourcing strategy increasingly leans towards a disaggregated supply chain, are how to:

- Extract the best value for money and efficiency from its service providers across different service bundles and technology stacks ("towers", if using the nomenclature of SIAM and towers).

- Incentivise its service providers to collaborate to act in the best interests of the customer in delivering end-to-

end services that meet the customer's business objectives.

A few years ago, traditional single-source models were starting to be disrupted in favour of a move to more of a multi-sourced environment as the cloud model began to take hold. As a result, the government started to explore new collaboration models, including alliance contracting (*for background, see feature article "21st century sourcing: revolution or evolution", www.practicallaw.com/2-522-0133*).

Alliance contracting model

The Department of Health considered the alliance contracting model as a framework that would underpin a major IT and services transformation project for the NHS electronic staff record and the administration of the NHS pension scheme. This model, sometimes known as collaborative contracting, was an innovative initiative by the Department of Health to borrow a contractual structure and delivery model that had been widely, and successfully, deployed in Australia and New Zealand for the delivery of complex infrastructure and construction projects.

Under the alliance contracting model, the customer and service providers collaborate to develop the requirements for the project and to share exposure to the project outcome. The theory behind alliance projects is that they are suited to more complex projects with many unknowns, where the parties do not have the ability at the outset to set out their requirements (based on detailed service or product specifications) or to predict with confidence the outcome using traditional contracting models, and therefore where the cost of trying to transfer risk to suppliers becomes prohibitive. The Department of Health decided to explore if this model could be adapted for a complex IT transformation project.

Although the alliance contracting model was ultimately dropped for this particular project, there remain some useful principles to draw on which are increasingly being deployed in collaboration models for complex IT and business transformation projects today.

Some of the key features of an alliance contracting model are:

- A "no fault" or "no blame" culture.

- A good faith obligation between the parties.

- A joint management structure.

- Risk and opportunity sharing.

- "Best for project" decision-making processes; that is, decisions are made that are best for the project as a whole rather than decisions that are primarily intended to advantage a particular party's position or service.

The principle behind the "no fault" or "no blame" concept is that, where there is an error, defect in service or poor performance by or across different suppliers in connection with a project, the parties do not, as a first step, seek to assign blame and pursue contractual rights and remedies, but rather attempt to agree a remedy or solution which is best for the project. This principle is reflected as the "rapid resolution" or "fix first, settle later" principle in many governance and collaboration frameworks in sourcing projects.

SIAM and towers model

Although the government did not ultimately embrace the alliance contracting model for complex IT projects, it turned instead to the SIAM and towers model for a number of years for its largest outsourcing projects (*for background, see feature article "Sourcing 3.0: the rise of the intelligent customer?", www.practicallaw.com/1-608-7044*). This saw the advent of a separate collaboration agreement that all suppliers were required to enter into alongside their bilateral agreements with the relevant contracting authority for their particular tower or service bundle.

Unsurprisingly, the supplier market has been reluctant to accept collaboration agreements or regimes where financial risk or reward is contingent on the behaviour of other suppliers, including by claiming against each other if particular dependencies are not fulfilled. Subsequent shifts in the government's approach to managing multi-party outsourcing have seen the SIAM and towers model fade from the spotlight (*https://governmenttechnology.blog.gov.uk/2015/02/18/knocking-down-the-towers-of-siam/*).

Choosing a collaboration regime

The main challenge for customers in the current digital age of sourcing is how to design a collaboration model that incentivises the customer and its many and varied

suppliers to collaborate and how to enforce that collaboration (*see box "Collaboration principles"*). The key questions when looking at a collaboration regime are: the extent to which it should be binding; and whether there are formal incentives, whether contractual or financial, built in to encourage the different suppliers to work together and to disincentivise certain behaviours.

Another important question is whether the collaboration regime should be achieved through a multi-party arrangement and, if so, whether this should be a legally binding arrangement, or a less formal collaboration charter or "captain's table" type arrangement. Alternatively, whether it could be achieved through a more traditional combination of collaboration mechanisms and features built in to the various bilateral contracts between the customer and each supplier, including through the use of more traditional non-binding operating level agreements that set out the various hand-offs and dependencies by and between each of the suppliers involved in a project or particular supplier ecosystem.

Whatever the desired approach, it is crucial that the customer "owns" the design and implementation of the collaboration regime. After all, if the customer does not appear to believe in, or be incentivised by, the collaboration regime, there is little chance that its suppliers will be.

It is clear that there is no one-size-fits-all approach to choosing a collaboration regime, and what works for one project, customer, supply chain or ecosystem will depend on a range of factors, including:

- The particular sector and culture of the organisation, including whether it operates in a regulated sector.

- The identity and sophistication of the suppliers.

- The complexity of the project or multi-seller environment.

- The maturity and experience of the customer's retained organisation and its SIAM function in managing the collaboration regime.

Changing role of the customer
Equally important in any collaboration regime is the recognition that the customer plays a vital role in the success of any collaboration

Collaboration principles

Whatever the contractual model, the following principles are vital to the success of any collaboration regime to which suppliers may be asked to adhere, as part of any project or multi-seller environment:

- Seamless and effective delivery of capability to end users or customers.

- Placing customer or end-user experience at the centre of service delivery, integration and issue and problem resolution.

- A "one-team" approach to service delivery, where parties collaborate towards shared outcomes.

- A rapid resolution and "fix first, settle later" principles.

- Collaborative governance and incentivising individual employees to adhere to the principles.

and an acknowledgement from the customer that there must be some customer accountability and investment.

The nature of sourcing in a more complex world of cloud, software-as-a-service and new technologies, means that the traditional outsourced model and form of contract, in which as much of the delivery and integration risk was passed over to the supplier as possible and "priced-in", is no longer viable in the new world of multi-tenanted solutions and shared delivery platforms.

In the sourcing and procurement contracts of today, a customer is much less likely to be procuring a system or solution that is bespoke, proprietary, dedicated or on-premise, or built to the customer's unique specifications. As a result, it is much harder for the customer to insist on contracting on its own preferred customer terms and conditions for delivery of the services or solution. Under previous bespoke deals, where the supplier had more end-to-end control over the design, delivery and operation of the end-to-end service or solution, it may have been more inclined to negotiate on the basis of the customer's terms and conditions and build risk into its pricing model, as appropriate.

However, ever since the cloud and other multi-tenant or shared platform models entered the sourcing scene, there has started to be a rebalancing of the relationships dynamic between customer and supplier, as customers realise that there needs to be a trade-off between insisting on all the traditional protections and clauses in its traditional

sourcing contracts, and embracing the "one-to-many", more commoditised, benefits of cloud-based service offerings.

Nevertheless, while disruptive technologies continue to change sourcing strategies and business models from an operational, delivery and commercial perspective, the evolution of the contracts that sit behind these new solutions and delivery models, as well as relevant laws and regulations, has been much slower.

New contract models
Customers and service providers are beginning to find a middle ground on the starting point for relevant contract terms. However, advisers need to work with both the customer and the service provider community to develop contractual frameworks which are more adaptive and responsive, often with an increased focus on outcomes, and which are more suited to the risk profile of delivery and shared platform models built around the cloud, "anything-as-a-service" (XaaS), intelligent automation and AI solutions. In particular, some of the former boilerplate sections of outsourcing contracts, such as relationship management, governance and record-keeping, have stepped forward as key provisions for addressing these new challenges.

The nature of many of these new delivery models mean that integration risk often remains with the customer and there will be increasing dependencies or other obligations on the customer, including by procuring that other suppliers in its supply chain do certain things.

Exiting services

As customers continue to embrace disaggregation and multi-sourcing, one of the effects is a cycle of regular re-procurement of, and exit from, existing services. Sometimes this will be as straightforward as on and off-boarding suppliers on a one-to-one basis. However, exit and transition regimes should generally ensure that they address:

- In-life requirements that relate to exit, including the maintenance and provision of exit information, and the role of both parties in exit readiness.

- Changes in the combination of services sought by the customer, meaning that exit from one contract may not map directly onto the implementation of one or more successor contracts.

- Staggered or multiple exits during the term of a contract.

- The role, if any, that the supplier will play in supporting the customer to procure successor services.

- The repatriation of some services to the customer.

- Risks arising from the cleansing and migration of data from the outgoing to the incoming supplier.

- Service or equipment becoming outdated or obsolete, especially in the context of end-user computing contracts where a new supplier coincides with a major technology refresh programme.

Exit schedules are often left as last-minute agreements to agree in order to secure a deal, but exit should be far from an isolated part of a sourcing deal. Instead, effective and efficient service transfer in multi-source and data-rich environments is of critical importance to enterprise IT management.

Customer organisations are becoming increasingly concerned about the capability of potential suppliers to deliver exit. This is matched by increasing scrutiny of suppliers' exit capabilities during procurement phases, whether run under public procurement rules or in the private sector. It is not uncommon to see a potential supplier's exit and transition capabilities being used as a differentiator among otherwise similarly credentialed bidders.

In more complex procurements, the exit and transition schedule (or equivalent) has grown from being a short, fairly operational product description of an exit plan accompanied by some generic obligations to a fully-fledged set of service requirements, obligations, performance standards and, as appropriate, specific remedies that can be triggered during an exit period. Customer organisations are also looking at ways to tie payments for exit assistance to achieving certain pre-specified exit outcomes or deliverables to ensure that the supplier remains adequately incentivised. This can be described as the so-called "exit-as-a-service" mentality.

One way of doing this is to agree pre-priced exit deliverables and milestones for certain aspects during the exit and transition cycle. To the extent that these can be codified in the contract or, failing that, exit plans, this can help to de-risk exit and ensure that both parties are on the same page when it comes to the scope and success criteria for exit, especially where the customer organisation is likely to be managing multiple exit and transition activities across a number of contracts.

Suppliers are usually also keen to standardise their exit offerings across their customers. For commoditised services there may be an off-the-shelf exit package that suppliers are willing to offer customers (sometimes with pre-priced components or other mechanisms to ensure cost certainty), with obligations carefully circumscribed and any add-ons priced on a time and materials, or similar, basis.

These need to be managed collaboratively and reflected appropriately in the contract, in terms of liability and risk transfer provisions (*see "Managing integration risk" above*).

Contracting, as well as relationship management and collaboration frameworks, need to evolve to keep pace with the rate of technological change. This will help to ensure that contractual structures remain fit for purpose, match the solution and service being delivered, and can help parties to proactively and flexibly govern complex delivery models in today's digital era. This will include dealing with key areas such as integration risk, change, dependencies, collaboration, governance, exit and re-procurement.

"Fit for purpose" from a governance and relationship management perspective might mean that these frameworks are more geared to: the "one-team" approach to service delivery, where parties collaborate towards shared outcomes; more agile working practices; and more openness, trust and transparency in the arrangements. Parties will also need to plan better for the entire contract lifecycle and, especially, exit (*see box "Exiting services"*).

THE FUTURE

Demand by customers for innovative solutions in the digital age has led to the disaggregation of service models and the increasing complexity of contract structures.

Disruptive forces on the sourcing market are compelling customers and suppliers to go back to the drawing board to ensure that commercial and contractual models are fit for purpose and adaptable in the face of change. As a result, customers and suppliers need to work collaboratively together to make a more diverse range of outsourced, in-sourced and increasingly co-sourced services work for the benefit of end users, clients and customers.

In the face of more complex supply chains, increasing data breaches, and cyber and security risks, the retained ICF needs to become even more intelligent and sophisticated in order to manage the challenge of end-to-end service integration across a disaggregated supplier ecosystem.

Throughout all of this, advances in technology and the continued rise of data as currency and its emergence as a vital asset for organisations in every sector (often serving as a cornerstone for an organisation's strategy), continue to challenge businesses to innovate to compete.

In revisiting their sourcing strategies, customers are appreciating that it is not just the bottom line that matters where, in the past, outsourcing used to be primarily concerned with cost savings and reduced headcount. Instead, as more and more customers take back control over their sourcing function as a means to fully exploit the benefits of business-transformative new technologies, there is an increasing awareness of the importance of properly integrating collaboration, end-to-end performance and the role of the integration function (SIAM or otherwise) into all aspects of service implementation, delivery and exit.

The sourcing market is changing or, more accurately, is more visibly having to respond to change and disruption. Far from being on its deathbed, the sourcing market is evolving into a more sophisticated, multivariate one. Customers and suppliers need to collaborate more to make a success of this, especially when responding to disruptive technologies and alternative delivery models.

Lawyers and advisers are being asked to help clients, both customers and suppliers, to build new commercial frameworks, and contractual and governance structures, that respond to these exciting developments in the sourcing marketplace.

Nick Pantlin is a partner, and Jeremy Purton, Alex Cravero and Claire Wiseman are senior associates, in the TMT, Data & Sourcing team at Herbert Smith Freehills LLP.

Related information

This article is at practicallaw.com/w-015-2058

Other links from uk.practicallaw.com/

Topics

Information technology	topic/5-103-2074
Outsourcing	topic/0-202-2707

Practice notes

Cloud computing	8-505-4625
Cloud computing: outsourcing and tower services	7-565-0045
Cybersecurity Directive: UK implementation	w-013-8329
Data security under the GDPR	w-013-5138
Demystifying artificial intelligence	w-008-5369
Due diligence in outsourcing	2-381-2359
Main issues in outsourcing contracts	6-107-4775
Main issues in software licensing and maintenance contracts	7-107-4789
Main issues in systems integration contracts	2-107-4777
Multi-jurisdictional outsourcing	6-219-3961
Offshore outsourcing	6-216-7962
Outsourcing: overview	2-202-1226
Overview of GDPR: UK perspective	w-013-3757
Service levels and service credit schemes in outsourcing	1-211-9964
Software as a service (SaaS)	7-385-1503
Special issues in IT outsourcing	6-372-6005
Subsequent generation outsourcing	7-366-4035

Previous articles

Artificial intelligence: navigating the intellectual property challenges (2018)	w-015-2044
Data use: protecting a critical resource (2018)	w-012-5424
Algorithms, apps and AI: the next frontier in discrimination law (2018)	w-013-8054
Blockchain and IP: crystal ball-gazing or real opportunity? (2017)	w-010-1622
General Data Protection Regulation: a game-changer (2016)	2-632-5285
Sourcing 3.0: the rise of the intelligent customer? (2015)	1-608-7044
Big data: protecting rights and extracting value (2015)	1-595-7246
Data transfers in the cloud: the struggle for compliance (2014)	8-581-9685
21st century sourcing: revolution or evolution? (2012)	2-522-0133
Outsourcing: is your contract a liability? (2010)	1-502-7777

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355