KEMP IT LAW

IT Law at the Apex

DIGITAL TRANSFORMATION

White Paper

Legal Aspects of Digital Transformation

Richard Kemp and Deirdre Moynihan

September 2020

LEGAL ASPECTS OF DIGITAL TRANSFORMATION: TABLE OF CONTENTS

CHARTS

LEGAL ASPECTS OF DIGITAL TRANSFORMATION

A. INTRODUCTION

1. **Introduction, scope and purpose**. This white paper is a collection of the individual blogs we have written as introductory and companion pieces to the segments of our Digital Transformation Webinar on 10 September 2020:
   - The 6 'E's of the digital transformation journey (Section B);
   - Key features of the digital transformation legal landscape (Section C);
   - Market update – key digital transformation issues in telecoms, cloud, software and services contracts (Section D);
   - Managing cybersecurity, data protection and other data risks and liabilities (Section E); and
   - Governance and best practice on the digital transformation Journey (Section F).

B. THE 6 'E'S OF THE DIGITAL TRANSFORMATION JOURNEY

2. **Introduction**. Ask 5 different businesses what the phrase "Digital Transformation" (in this paper, '**DT**') means to them and you're likely to get 5 different interpretations. It's one of the most popular phrases used in connection with technology projects – a quick Google search for the phrase results in around 41 million hits! It's the hot topic of the year and COVID-19 has buoyed the market for new technologies and new ways to do business in unanticipated ways, including: the decline of cash and move to card/mobile payments, businesses moving to video conferencing and other quick and easy ways to communicate online, increased scrutiny of IT infrastructure and cybersecurity, and increased demand for data, analysis and AI, to name but a few.

3. **DT end goals**. DT can be anything from:
   - "IT modernization (for example, cloud computing), to digital optimization, to the invention of new digital business models" in Gartner's[1] terms;
   - to "organizational change through the use of digital technologies and business models to improve performance" in the words of the Global Centre for Digital Business Transformation;[2] and
   - to Wikipedia's description[3] of it as the "use of new, fast and frequently changing digital technology to solve problems. It is about transforming processes that were non digital or manual to digital processes".

   From those 3 descriptions, we see that DT is about a number of different end goals, including:

   (1) updating end of life/redundant systems and infrastructure;

   (2) moving to the cloud and XaaS (everything as a service);

   (3) using big data, AI and machine learning for analytics;

---

[1] See https://www.gartner.com/en/information-technology/glossary/digital-transformation.

[2] See page 3 of the Conceptual Framework for Digital Business Transformation, published by the Global Centre for Digital Business Transformation, a CISCO and IMD initiative, at https://www.imd.org/uupload/IMD.WebSite/DBT/Digital%20Business%20Transformation%20Framework.pdf.

[3] https://en.wikipedia.org/wiki/Digital_transformation.

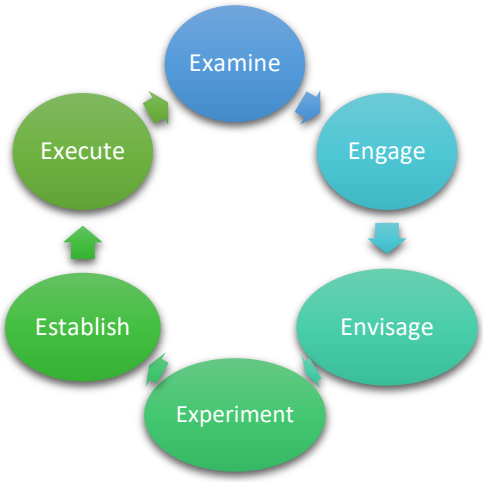
(4) creating and using new technologies such as IoT connectivity, automation, blockchain, cryptotech and Web 3.0; and

(5) (more generally) using technology efficiently and effectively to save costs and increase revenue.

Looking at DT through that "end goal" lens focussed on the delivery and implementation of new technology is overly narrow, however. Fundamentally, DT is a continuing and changing journey to improve business processes, operations, engagement, productivity and revenue through the use of new technologies. It can happen organically through internal development, involve the acquisition of new technologies or result from a cross functional or business collaboration project.

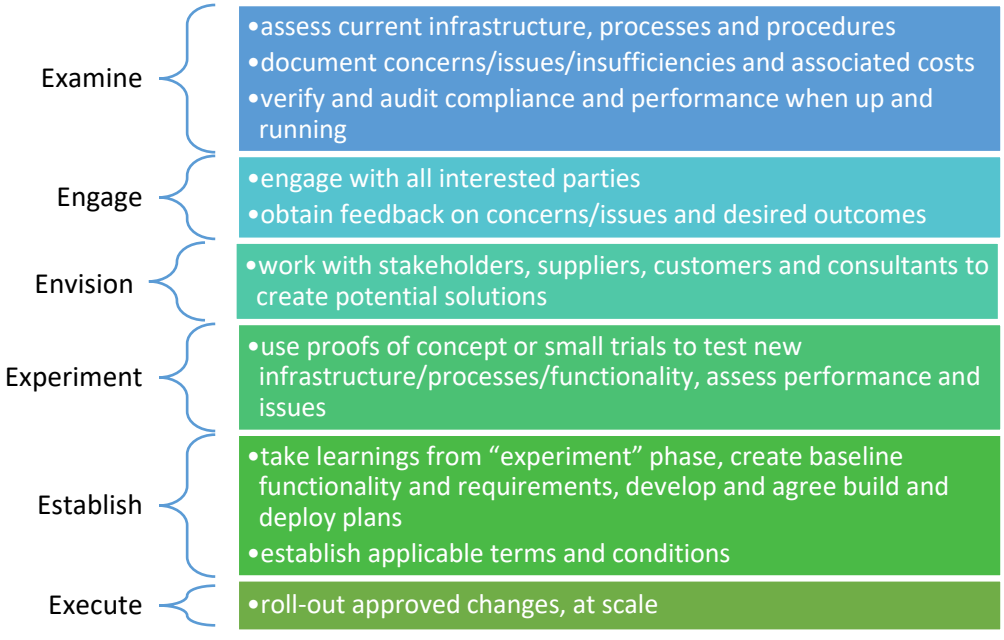
4. **DT and the 6 'E's: Examine, Engage, Envisage, Experiment, Establish and Execute**. All organisations, whether consciously or not, are therefore at one or more stages of the following DT journey:

Chart 1 –The 6 'E's of the digital transformation journey



Elaborating on those 6 elements, it's important for businesses to analyse and execute the various steps described below in an agile manner:

Chart 2 – The 6 'E's: Examine, Engage, Envision, Experiment, Establish, Execute

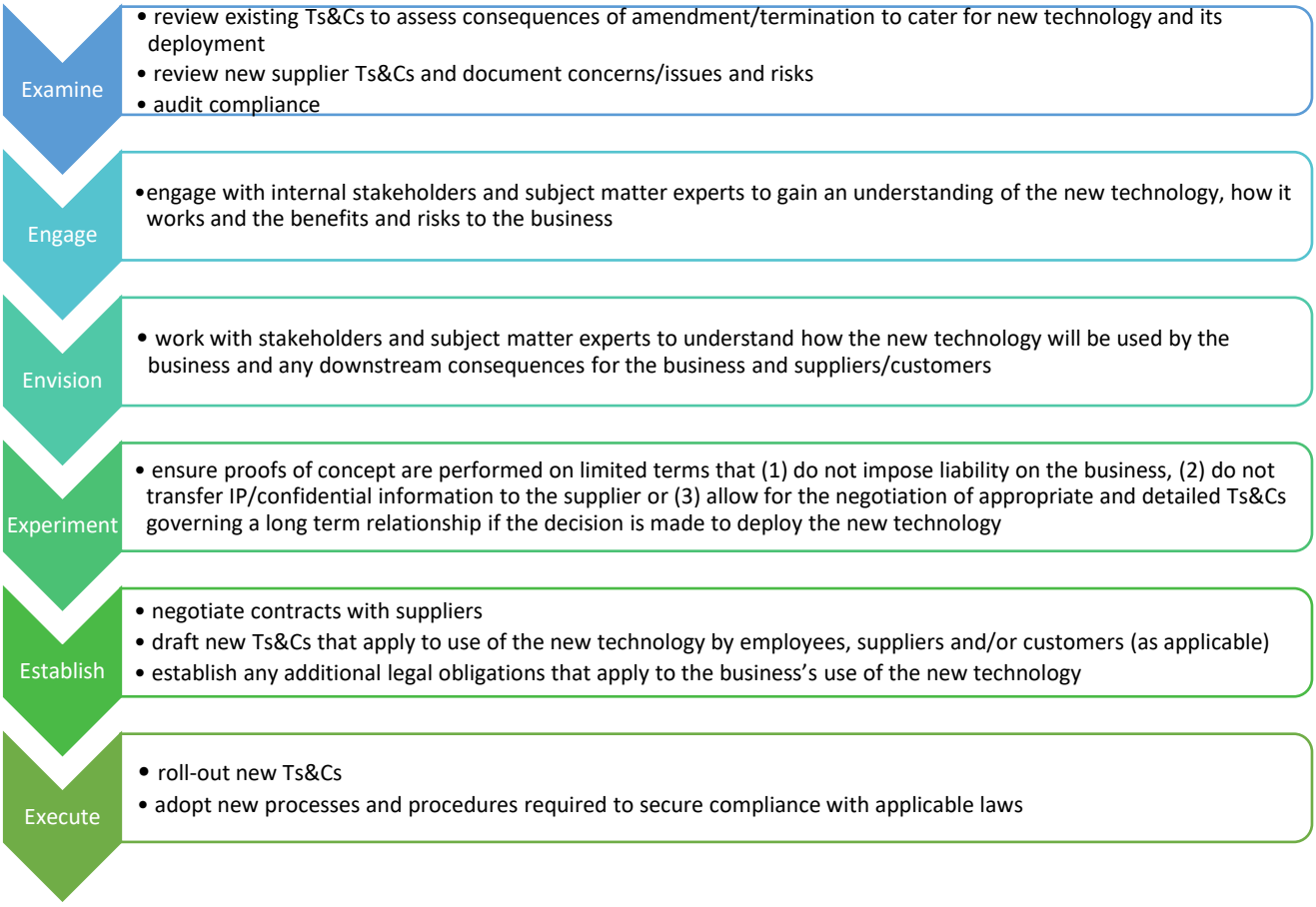


Each element will differ in relative importance from project to project but any successful project should be divisible into each of these individual elements.

5. **The 6 'E's from a legal perspective**. Research from Business Europe in 2017[4] indicated that "less than a third of the surveyed companies significantly involve their legal department in the strategic planning of digitalisation". This statistic sits uncomfortably with the fact that the same respondents in the same research project also stated that legal issues around the cloud, data ownership, liability and access to data were key concerns applicable to the deployment of new technologies in their businesses.

   From a legal perspective, those 6 elements are also relevant and, if followed, should reduce legal and business risk associated with any new DT project. For the lawyers, the 6 elements mean the following:

Chart 3 – The 6 'E's from a legal perspective



6. **Elements 1 to 3**. Elements 1 – 3 are all about clarity – describing the destination, explaining what the journey looks like and any potential hurdles along the way. Detail here makes it easier for the lawyer to usefully answer the "can we do this?" or "what do we need to do to do this?" questions.

[4] See page 10, Legal issues of digitalisation in Europe, measures to effectively help companies advance their digital strategies, available at https://www.businesseurope.eu/sites/buseur/files/media/reports_and_studies/2017-09-29_legal_issues_of_digitalisation_in_europe.pdf.

7. **Elements 4 to 6**. Elements 4 – 6 are all about detail – How will it work? What do we need to do? What are the key considerations for the business? What suppliers are performing what tasks? What laws/obligations are we subject to? What's our liability?

8. **The legal team as part of the business group**. In our experience, having the legal team join the broader business group throughout the journey helps reduce issues and/or disputes regarding:
   - rights in relation to data – access, use, control;
   - ownership and use of existing and new intellectual property rights;
   - confidentiality and trade secrets, particularly relevant for business processes;
   - risk management – liability of suppliers, to customers, to regulators;
   - regulatory issues – GDPR, sector specific regulation; and
   - performance and service levels.

   Consulting the lawyers may also add clarity by helping to identify additional costs or unanticipated issues that may delay time to contract or time to launch by examining the consequences of the intended use of the new technology – in their drive to deploy, innovators within businesses may gloss over "minor" details or obscure complexities that in actual fact are vital elements of the legal risk and compliance analysis that ultimately serves to protect the business.

   Ultimately, the journey is not one that the business, IT or legal teams can take individually and in isolation. It's therefore key to involve the lawyers at the appropriate time during each element of the project, particularly where sign-off from the in-house legal team is required to green light the project.

C. DIGITAL TRANSFORMATION: KEY FEATURES OF THE LEGAL LANDSCAPE

9. **Defining DT.** Nebulous and potentially boundaryless, DT can be challenging to articulate clearly. Diving in, we'll define it broadly as the investment in technologies, people and processes by an organisation to optimise its digital business capabilities. To make it more manageable from the legal perspective, we'll distinguish between digital transformation as the *journey* and digital business – enhancing customer experience and competitive advantage – as the *destination*. This white paper focuses on the DT journey.

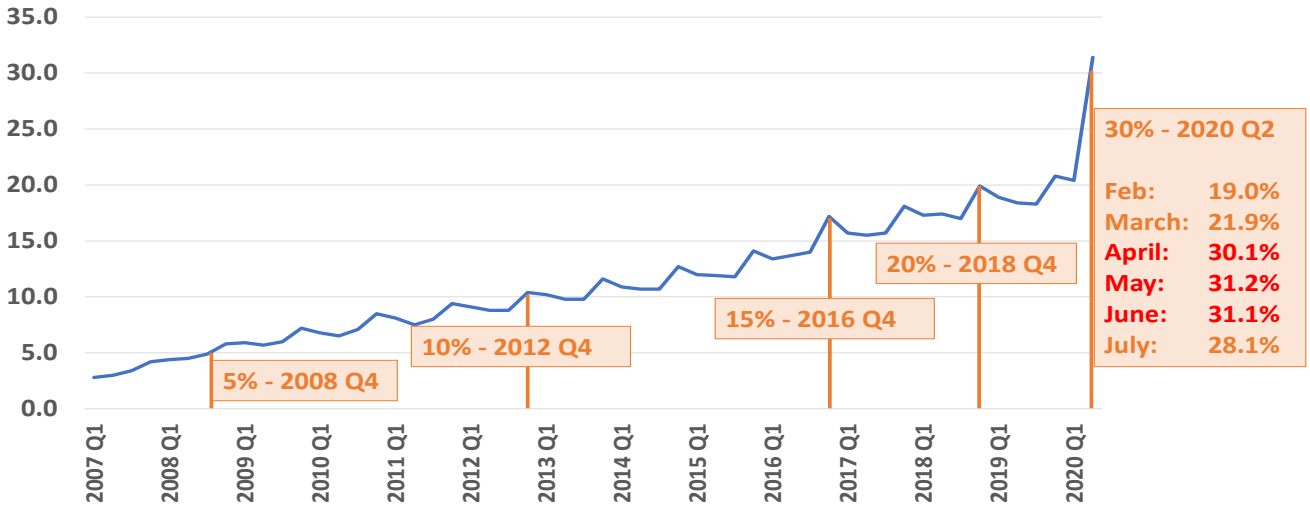
10. **DT was the top IT priority even before the Covid-19 pandemic struck**. Even before the pandemic hit, DT had emerged as the top priority in the organisation for technology initiatives in 2020, with (in roughly decreasing order):
    - cloud as key DT journey enabler;
    - a much clearer focus on cybersecurity, data protection, compliance and governance;
    - increasing investment in data analytics and machine learning; and
    - 'always on' software development through DevOps and IT service management as a service.[5]

11. **The pandemic has accelerated these trends in a way unforeseeable at the start of 2020**. The COVID-19 pandemic has accelerated these trends in a way unforeseeable at the start of 2020. How UK internet retail sales have grown illustrates this well. Taking internet sales as a proportion of total UK retail sales, it took four years for online sales to double from 5% to 10% (2008 to 2012), and another four to get to 15% (Q4

[5] See for example Flexera 2020 Digital Transformation Planning Report, page 3.

2016). But it then took only two years to reach 20% (Q4 2018). In April 2019, Mr Mark Carney, Bank of England Governor, was saying "last year one fifth of all sales in the UK were online. Next year, it will be one quarter"[6]. In fact, as Chart 4 shows, it has taken just eighteen months to get from 20% to 30% (Q2 2020).

Chart 4 - Internet sales as a percentage of total UK retail sales, 2007 – 2020 (Source: ONS)



12. **Retail as proxy for other sectors**. At the macro level, the combination of strong internet growth in 2018 and 2019, physical retail lockdown and a hefty shove online in 2020 is behind these figures. The acceleration of these trends in the high street stands as proxy to other sectors, whether the pandemic is a challenge (travel, leisure, hospitality) or an opportunity (healthcare, financial services), as well as to other walks of life, like legal services, where DT is starting to make a real difference.

13. **The cloud as DT enabler**. DT isn't occurring only in vertical sectors however. The cloud is a powerful DT enabler, whatever the sector. And horizontal areas that until very recently were the province of large numbers of human boots on the ground are now being cloudified and automated. Nowhere is this more pronounced than in cybersecurity, where automating incident detection and response, privileged access management and data loss prevention is starting to remove some of the compliance and governance headaches, or at least enabling them to be managed in a more structured, proactive way.

    What are the key legal features of this rapidly transforming digital landscape? We can break them down into two – key *DT lawyering* 'do's' and 'don'ts', and key *DT deal* 'do's' and 'don'ts'.

14. **DT lawyering 'do's' and 'don'ts'**. On the DT lawyering front, and as DT projects take up more of an organisation's resources, it's all about clarity, scope definition, relationships and objectives. From our seat deep inside the fourth industrial revolution, the range and speed of adoption of new IT techniques rippling out across business can appear daunting – 5G, Web 3.0, Smart APIs, AI/ML, IOT, DevOps, blockchain, cloud and mixed reality to name but a few. But getting to clarity around what the tech does is an essential first step towards being able to scope it out and apply legal principles to it: clarity of legal analysis based on genuine understanding of the tech is a prerequisite for the team effort.

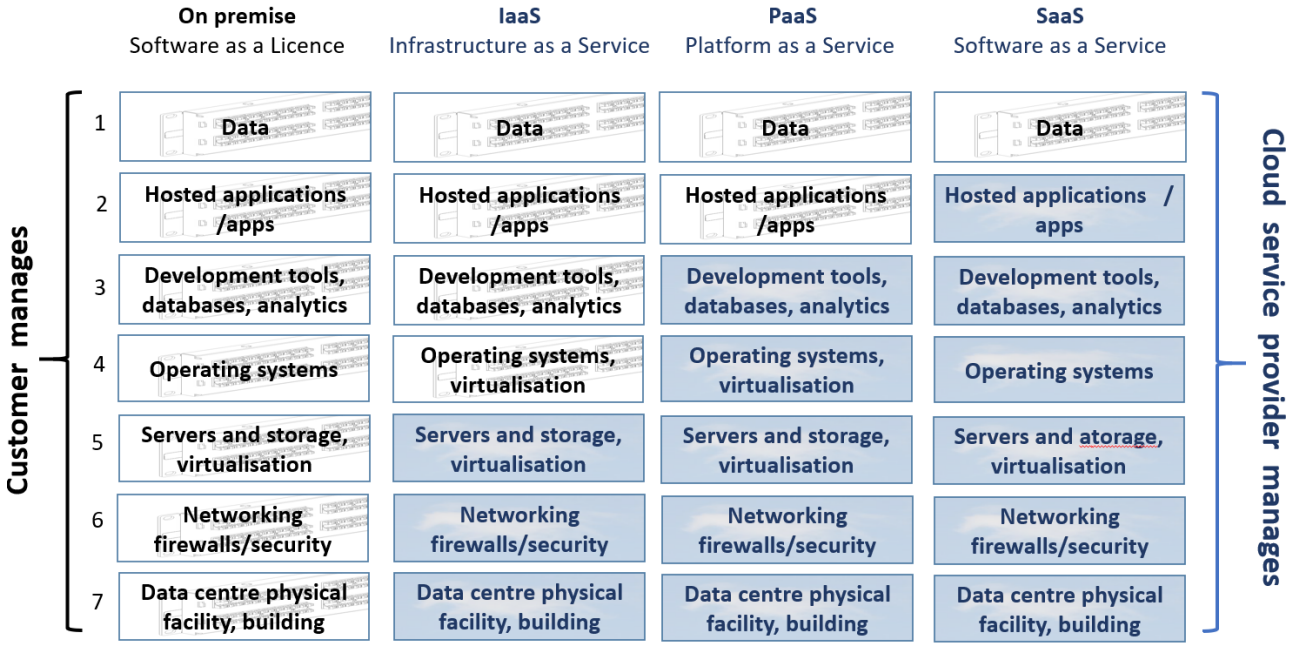
[6] '*A Platform for Innovation*', speech given by Mark Carney, Governor, Bank of England at Innovate Finance Global Summit, London, 29 April 2019.

Along with understanding the tech goes the legal team's stakeholder role in helping shape the organisation's strategy, policies and processes around DT, particularly in the areas of designing in compliance (privacy and data protection, cybersecurity, sector specific regulation), end to end data governance and DevOps' 'always on', shortened software life cycle. Writing up the foundational documents – from the vision, through the policy to the detailed processes – clearly and concisely and communicating them effectively enhances buy-in across the organisation.

15. **DT deal 'do's' and 'don'ts'**. The legal team's role in DT compliance and DT deals gives it an enabling role in managing DT projects – whether strategic or tactical deals or strategic compliance – and in setting agendas and objectives.

    On the DT deals front, cloud due diligence, procurement and contracting are now in the mainstream, but as we move to 'everything as a service' (XaaS), understanding the basics of the different cloud service models (SaaS, PaaS and IaaS) and delivery models (public – a room at your hotel; private – my own room; and hybrid - combination) remains the first step (see Chart 5).

Chart 5 – The cloud continuum



16. **Effective contract management is critical in DT projects**. As the business models and contracting approaches of the major SaaS players mature, it's becoming increasingly common on a single larger DT project to deal with the core SaaS provider, the professional services implementation partner and one or more providers of contiguous services. How the customer defines scope and shapes the contract structure is critical. It may be impractical to get all parties involved to sign up to one contract, but in a series of bilateral contracts, aligning the dependencies between different providers puts a premium on effective contract management. Establishing from the outset a common approach to project methodology, reporting standards, testing and structuring relief events can make all the difference here. In passing, AI as a Service (AIaaS) deals are becoming increasingly popular and aligning the customer's and the provider's ethics and data policies can be a challenge.

17. **A coherent and consistent approach to data is key**. A coherent and consistent approach to data in DT deals is also key. We're not just talking about data protection and cybersecurity compliance – key though they are – but also a more standardised approach to data governance that looks at data both as corporate asset and as a source of potential risk or liability.

18. **DevOps**. As software development moves centre stage, with many organisations using their own apps and APIs in enhancing the customer experience, we're moving away from the structured, sequential waterfall model, past Agile and towards DevOps, combining shorter development cycles (Dev) with continuous operational (Ops) delivery. In this world, effective internal policies around the following are key:
    - *software asset management*: ensuring proprietary third party software is used within licence scope;
    - *open source software ('**OSS**')*: managing residual risk around copyleft and OSS deployment; and
    - *source code management*: source code repository like GitHub for the software the DevOps team writes.

19. **Growing importance of lawyering DT**. Lawyering DT is becoming a core part of the organisation's skillset in successfully responding to the great shove online, and lawyers' unique combination of skills – getting to grips with the technology, applying evolving legal principles to how it's contracted for and used, formulating strategy and policy, helping assess risk, communication and relationship building – will continue to play an important role in ensuring that success.

D. MARKET UPDATE: KEY DIGITAL TRANSFORMATION ISSUES IN TELECOMS, CLOUD, SOFTWARE AND SERVICES CONTRACTS

20. **Introduction**. On any given DT project, there are numerous potential issues and pitfalls that may lead to failure – or at the very least – result in the project failing to meet the "on time, on budget and to standard" threshold. This section focusses on 3 key issues that arise on every DT project: (1) early adopter risk v. reward, (2) "toothless" functional and service standards, and (3) responsibility for/relationship with third parties and other service providers.

21. **Early adopter risk v. reward**. Very few customers want to be the first to purchase new software or deployment models – people naturally gravitate to suppliers, products and services that are tried and tested, as evidenced by success stories and positive feedback. The recent great shove online and the speed of deployment of new digital business methodologies means that it's not always the case that another company has "been there, done that and bought the t-shirt" for DT projects. Customers are therefore, at present at least, slightly more nervous when undertaking a DT project simply because the supplier may not be able to refer to a number of successful deployments or successfully point to issues that have arisen and been quickly and efficiently addressed with minimal impact to the customer.

    This lack of confidence – and potential inability to foresee problems – means that customers are likely to assume increased risk of failure in scenarios where the supplier is unlikely/unwilling to offer additional protection/legal rights to the customer.

    To mitigate these risks, it's important to ensure that:

    - the contract includes meaningful commitments from the supplier as to what it will deliver and that delivery will be "on time, on budget and to standard" (see paragraph 22 below for more details);
    - the customer has meaningful and enforceable remedies to address failures to avoid incurring irrecoverable additional expenses and losses (see paragraph 22 below for more details);
    - the enthusiasm and positivity of the supplier in relation to its newer offerings is tempered by enforceable contractual provisions that actually assist the customer should issues arise. It may be

tempting to rely on the supplier's experience and statements made during procurement and pre-contract negotiations, market position or the nature of the relationship between the parties as sufficiently persuasive for the customer to remove the need for detailed contractual terms around fixes issues and dispute resolution. The disadvantage with this approach is that any change in the relationship or the supplier's approach means that the supplier's word is no longer its bond and the customer may be without a remedy. For this reason, we always advise that the customer vet and assess the nature of the remedies available to it for different types of breach so that it is confident that the contract provides sufficient protection, irrespective of the quality of the parties' relationship and the issues that may arise.

22. **Functionality and performance commitments**. It's easy to be swayed by enthusiasm and marketing spin about the benefits and functionality of new technologies and how those technologies will deliver efficiencies and performance improvement for the customer. There's usually a relatively large disconnect between pre-contractual statements around functionality and performance and what the contract requires the supplier to deliver: it's commonplace for customers to ask for suppliers to confirm that its product/service includes specific functionality on an item-by-item basis but for the contractual commitment for the supplier to state that the product/service will perform "in all material respects in accordance with" the supplier's high level, generic, product/service description. This approach makes it more difficult for customers to have a clear contractual hook on which to hang allegations of breach or failure to perform. It's therefore important that the parties address these issues during the contract negotiations and the risk can be mitigated in the following ways:
    - Any requirements list that has been prepared by the customer reviewed by the supplier during the RFP should be included in the contract as a baseline expectation of functionality/performance.
    - Proofs-of-concept can be used to test functionality and performance against the supplier's standard commitments and the customer's requirements list.
    - Formal, official acceptance by the customer should ideally be based around successful completion of user acceptance testing by the customer and a period of live, production use without P1 or P2 priority issues.
    - Remedies for failed acceptance test/breach of commitment to deliver functionality/requirements should be assessed by reference to the potential impact of a failure and any resultant delay. It's unlikely that the supplier's standard approach of a "fix/replace commitment" as the customer's sole remedy will compensate the customer for any wasted costs and additional expenses it may incur because of the supplier's failure to deliver on time and to standard. Liquidated damages, or the ability to recover operational losses and additional costs/expenses, may go some way to re-balance the risk here but it's unlikely in our view for the customer to have carte blanche to sue for all loss/damage and/or terminate the agreement in these circumstances.

23. **Relationships with third party providers**. No DT project is completely ringfenced such that it can be implemented without interaction with, or support from, other third party service providers to the customer and/or the supplier. The transformative nature of the DT journey means that a change to one element in the IT stack (as illustrated in Chart 5 above) is likely to impact other layers/elements within the technology ecosystem. This cross-party dependency can easily be overlooked by a blinkered focus on one supplier or one system/service at a time and that narrow "worldview" of the impact of each individual "DT project" can result in increased complexity and additional cost and expense for all parties involved. It's not unusual in our experience for both customers and suppliers to overlook downstream consequences on other suppliers and to fail to identify early in the implementation process when support and input from other

suppliers is required. The project plan/governance methodology should therefore incorporate processes designed to:

- Identify all impacted suppliers/service providers to both customer and supplier and what support/assistance/input is required of those suppliers/service providers.
- Address who is responsible for managing the third party and the consequences of a failure to do so.
- Ensure that the supplier is responsible for the acts and omissions of its sub-contractors and service providers – be wary of force majeure clauses or other disclaimers buried within documentation which operate to remove/reduce the supplier's liability because of a breach by/failure of its sub-contractor or service provider. This is particularly key in cloud and "as a service" deployment models where suppliers routinely seek to exclude liability for third party failures by declaring them to be force majeure.

24. **Be SMART**. Ultimately, the points we've discussed in paragraphs 21 to 23 above are intended to assist both parties during any DT project. Fundamentally, we're advocating a SMART approach to a DT project where each party is aware of the detail, intricacies and risks associated with the project and commits to SPECIFIC, MEASUREABLE, ACHIEVABLE, RELEVANT, and TIMELY contractual rights and obligations to successfully deliver it. Using these principles can help the parties ensure that both are acutely aware of what's required to deliver any DT project successfully "on time, on budget and to standard" and can also reduce scope of disagreement and conflict.

E. MANAGING CYBERSECURITY, DATA PROTECTION AND OTHER DATA RISKS AND LIABILITIES

25. **Introduction**. A quick Google search on data breaches/cyber security issues/GDPR investigations and fines results in hundreds of thousands of hits covering best practice guidance, scary facts and figures and detailed analyses of the causes of information security and data breaches. To illustrate:

- Gartner predicts that the worldwide information security market is forecast to reach $170.4 billion in 2022 (Gartner);
- 68% of business leaders feel their cybersecurity risks are increasing (Accenture);
- Hackers attack every 39 seconds (University of Maryland);
- 52% of breaches caused by malicious attacks and 80% affect personal info (IBM);
- It takes on average 280 days to ID and contain a breach (IBM);
- Total annual cost of cyberattacks is increasing (Accenture).

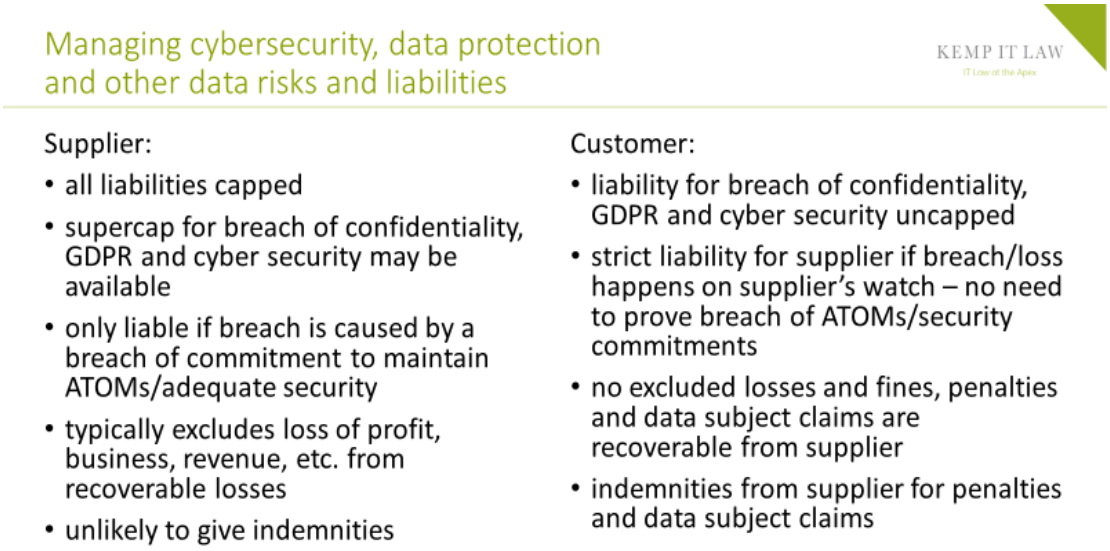
DT can both help and hinder cybersecurity and data management: new technologies monitor security threats in sophisticated and agile ways – "cybersecurity-as-a-service" (CaaS) is becoming more prevalent and can offer a simple, effective "one stop shop" approach to ensuring system security and integrity. Outsourcing CaaS, or indeed adopting state of the art cybersecurity hardware, software and processes, does not completely remove the risk of breach – like a chain, cybersecurity is only as strong as its weakest link.

26. **Contractual commitments**. Any DT project will therefore need to address cybersecurity contractually, by including terms stipulating: (1) the information security/cyber security standards that the supplier is obliged to meet – be they "appropriate and technical organisational measures" in GDPR-speak or other security standards, (2) that the customer can vet and audit the supplier's compliance with the contractually mandated standards, (3) the circumstances in which the supplier is liable for a breach/cyberattack, (4) the extent of a party's liability financially, and (5) what costs, expenses, losses and liabilities are recoverable.

27. **Liability**. Liability for cyberattacks/breach of GDPR/breach of information security commitments are a key focus for both customers and suppliers when negotiating the Ts&Cs for any DT project. The approach to cybersecurity issues has changed in recent years owing to the potential significant consequences of a GDPR breach and, for now at least, we see that treatment of breach of confidentiality, GDPR and information security obligations are addressed as one issue.

    The usual starting positions of both supplier and customer are illustrated in Chart 6 below. Typically, a negotiated deal will result in the parties agreeing some form of middle ground based on: (1) the nature of the data/information at issue (Does the supplier process sensitive "special category" data or financial data or more "low risk" personal data such as employee email addresses?), (2) the service offered by the supplier and how it uses the customer's data, (3) the committed revenue spend by the customer, (4) the customer's industry (Is it regulated?), (5) the risk posed to the customer resulting from a breach of security/confidentiality/GDPR committed by the supplier, and (6) market practice.

Chart 6 - cyber and data risks and liabilities



28. **Practical considerations**. The negotiation of the legal terms as described in paragraph 27 above should be based on a risk-based assessment in full knowledge of the roles of the supplier and customer and data flows and data uses. The following questions and considerations may help focus the discussions on key risks and concerns and no contract should be signed by the parties unless the following points have been addressed in one way or another:

    - Each party should understand what data it possesses and its role in relation to that data – is it a controller or processor for GDPR purposes? Are they joint controllers?
    - Is it possible for the supplier or the customer to override contractual commitments by choosing specific options within the software/service offered by the supplier?
    - If a breach occurs, what's the potential impact on the parties and any other individual or entity impacted by the breach? Is it a GDPR issue? Or a disclosure of confidential business information (e.g. financial reports, know-how, trade secrets)? Are fines possible? Can individuals or third parties make claims?
    - What is the supplier required to do in the event of a breach? Must it provide all assistance in a timely manner? Does it have a process for dealing with cyber/data breaches?

29. **Fix first, argue later**. If a breach arises, speed of response may be crucial as any delay may increase loss or liability. It's good practice, therefore, for the parties to adopt a "fix first, argue later" approach to addressing the consequences of a data breach. The parties should be permitted to take necessary steps to mitigate/reduce/remove the breach or cause of the breach in the most appropriate way possible based on what the parties view as the best approach without first having to assess potential contractual and legal liability. This is particularly key for "as-a-service" offerings where one breach of security for one customer may cascade through to other customers of the supplier. The supplier may therefore reserve rights to suspend access to all or part of the service to resolve this issue and may also take unilateral action where it believes it's required to reduce the likelihood of/avoid a breach. In suggesting these remedies and pursuing a "fix first, argue later" approach, we are not advocating for carte blanche for either party to do what it thinks appropriate in response to cyber incidents – the terms of the contract will still apply and each party will still be able to exercise its rights – we are simply suggesting that good governance requires the parties to attempt to resolve the incident while the lawyers review the applicable contractual terms!

F. GOVERNANCE AND BEST PRACTICES ON THE DIGITAL TRANSFORMATION JOURNEY

30. **Introduction**. Digital Transformation – the investment in technologies, people and processes by an organisation to optimise its digital business capabilities – was already top priority for CIOs in 2019, and has been accelerated in 2020 by the pandemic in a way few could have foreseen six months ago. The adaptation to working from home in response to lockdowns in the spring, the growth surge of BigTech since then, and innovation demonstrably moving from the lab to the mainstream have all contributed to a hefty shove online this year and a growing recognition that there really is no sustainable long term offline alternative.

31. **DT happens in flight!** But DT doesn't happen in a vacuum and takes place when the business is in flight, putting a premium on visioning the change and strategy, planning, governance and best practices around implementation. The legal team has a lot to contribute in each of these areas.

32. **Genesis of DT projects**. The genesis of DT projects is typically a report, highlighting (externally) how customer expectations are moving on and (internally) how current IT falls short: infrastructure may be nearing end of life; architecture may not address evolving security threats; IT resources may be deployed piecemeal and delay time to value; and limitations may lead to growth of shadow IT outside existing governance.

    Analysis will focus on (external) customer-facing objectives of enhancing engagement, experience and solutions and (internal) people-facing objectives of empowerment and communication, and the articulation of a coherent, unifying vision.

33. **The DT cloud journey and governance**. The cloud is the great enabler of DT, and the vision is generally implemented through cloud architectures (increasingly, public, private and hybrid), frequently at all levels of the cloud stack (data centre, network and server infrastructure; software platform; and software as a service) and integrating external and internal IT services seamlessly and speeding up time to value.

    Planning the organisation's cloud journey is critical and charting implementation is in many ways down to the nuts and bolts of effective supplier management. Very often, there'll be a consultancy piece at the outset around service definition and procurement, and the legal team should have a seat at the table where the details of each procurement and due diligence, timings, dependencies and risks between the individual constituent contracts are all assessed and aligned.

34. **Managing execution risk**. The dependencies in large scale DT projects can be a major source of execution risk. Some SaaS providers will use their own professional services ('**PS**') businesses for configuration, migration, sizing and deployment, but others will leave them to third parties, so you may have a number of different suppliers – existing system, new SaaS, PS and perhaps auditors – on just one project. SaaS projects may be preceded by a data centre, IaaS (infrastructure – networking, compute, storage, virtualisation) or PaaS (non-application software) project, and any delays or performance shortfalls in one of these may have a knock-on effect on the SaaS implementation, increasing time and costs. Where the output of a SaaS project is customer-facing, SLAs in customer agreements may be at risk through delays or failures elsewhere in the contractual ecosystem.

35. **Contract management framework**. DT governance arrangements should ensure individual projects are managed within an overall framework and, where sequencing, dependencies and relief events (delay by supplier A means that supplier B will also be late) are robustly managed. It may not be possible to get the customer's project methodology adopted by all parties, but common standards on, or at least a common approach to, reporting, information sharing and testing are critical. The legal team has a natural part to play in DT governance at each level, as well as holding the pen on the contract negotiations themselves.

36. **Data and risk**. GDPR compliance continues to drive governance and best practices in the area of personal data, especially in sharing data between organisations, where market practice is starting to be much more granular about the boundaries between processor and controller and, in the controller context, what constitutes a joint controller relationship. The striking down of Privacy Shield in July 2020[7] has led to a closer attention to international transfers and the Standard Contractual Clauses.

37. **A different lens: data value, cost, risk and constraints**. Whilst data protection is the foundation of data management, the widespread adoption of AI has added a multiplicity of AI ethics frameworks, governance models and best practice statements which can be confusing in practice. Looking at data governance in the round, organisations are increasingly analysing their data estate through the lens of policy considerations, based on data:
    - *value*: quality and quantity of data, measured by context and timeliness;
    - *cost*: of storage, curation, maintenance and disposal;
    - *risk*: based on data sensitivity classification; and
    - *constraints*: contractual, regulatory, privacy, IP, HR, commercial interests and societal.

38. **Risk assessment by use cases**. Looking through this lens, data use cases parsed in different ways:
    - between data that is '*human impacting*' and '*human non-impacting*';
    - between for data used for *input*, *processing* and *output*;
    - between data used *internally* and *externally*.

    Different sets of standards and automated checklists will then be applied to or prepared for different use cases segmented according to these criteria.

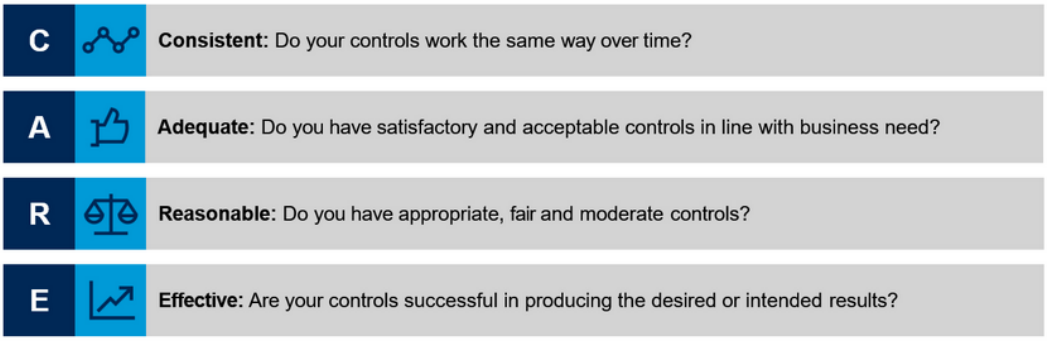
[7] Judgment of 16 July 2020 the European Court of Justice in **Case C-311/18**, *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*

39. **Cybersecurity and risk**. This busines risk-based approach to managing data and risk is also reflected in a more pragmatic, albeit outcome based, regulatory approach to cybersecurity. In an interview with the Wall Street Journal[8] at the time of the announcement of £99m Marriott and £183m BA fines in July 2019, the UK Information Commissioner was reported as saying:

> "Our focus is whether or not there was adequate, reasonable, consistent and effective data security to protect people's data … [W]e look at whether or not doors were left open to make it easy for cyberattacks, whether or not the attack was foreseeable, what kinds of due diligence and steps were taken in the data security program. … So many of our investigations are finding basic or a lack of cybersecurity hygiene, lack of some of the most basic protections that people would expect …"

40. **Gartner and the CARE standard – consistent, adequate, reasonable and effective**. Slightly rearranging Ms Denham's descriptors, Gartner has come up with:

Chart 7 – The CARE standard for cybersecurity



Gartner commented that:

> "[i]n these four characteristics are a myriad of opportunities to do what is best for the organization. It supports the creation of a balance between protection and running the business. It also embodies the incentive to build a better security capability that delivers better outcomes, not just spend more money on security."

This more practical approach will help inform organisations in their security due diligence assessments of DT providers.

41. **DevOps and risk.** It's 5 years since the CEO of Microsoft famously said that "every business will become a software business, build applications, use advanced analytics and provide Saas services"[9] but it's perhaps taken the rise of DevOps – combining shorter development cycles (Dev) and continuous operational delivery (Ops) – for this prediction to start to become a reality. As software development moves centre stage for business, and organisations increasingly use their own apps and APIs in enhancing the customer experience, effective internal policies around software asset management (ensuring proprietary third party software is used within licence scope), Open Source Software (managing residual risk around copyleft and OSS deployment) and source code management (manging the software that the organisation develops itself) are critical.

Kemp IT Law, Solicitors (Ref: RHK/DAM)
September 2020

---

[8] '*UK Regulator on Why It Is Pursuing Record Fines Against BA, Marriott*' Catherine Stupp, Wall Street Journal, 10 July 2019, referred to in '*The Urgency to Treat Cybersecurity as a Business Decision*', Paul Proctor, Gartner, 12 February 2020

[9] 'Satya Nadella: Every business will be a software business', Cliff Saran, Computer Weekly, 18 March 2015

KEMP IT LAW

IT Law at the Apex

Richard Kemp
Partner

T: 020 3011 1670
M: 07932 695 615
richard.kemp@kempitlaw.com

Deirdre Moynihan
Partner

T: 020 3011 1627
M: 07710 395 460
deirdre.moynihan@kempitlaw.com