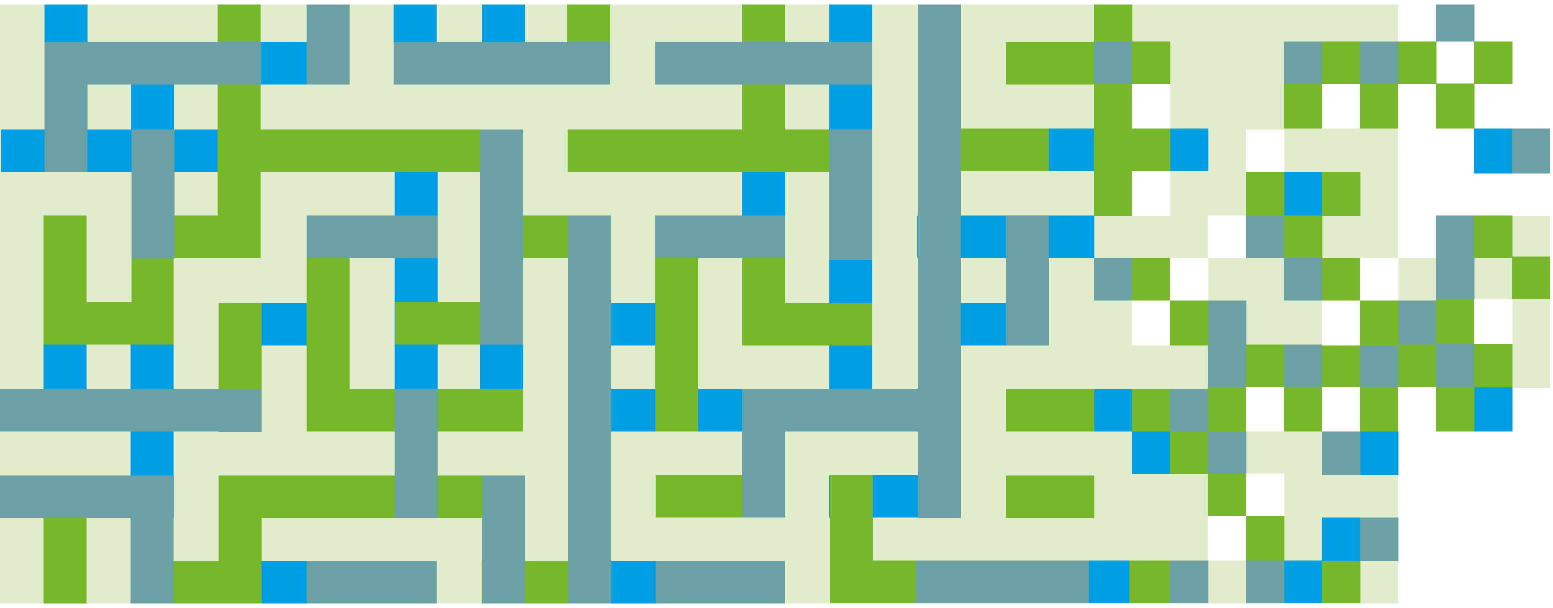
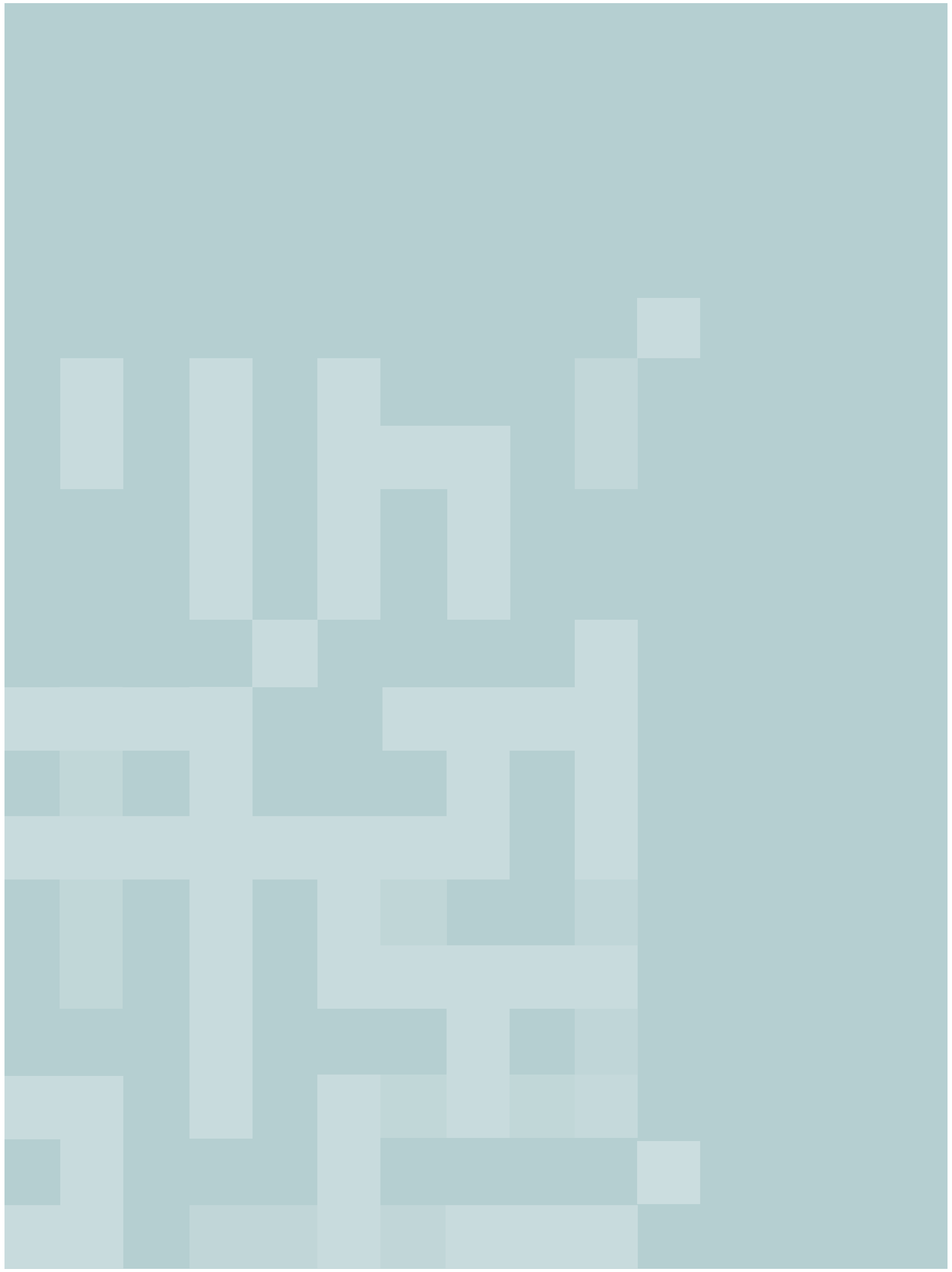
Linklaters

Microsoft

Lawyers: Agents of Change in a World of **Digital Transformation**

A joint publication by Linklaters and Microsoft





Foreword

Over the last 2 to 3 years, the focus on digital transformation by companies across all industries and countries has risen exponentially. We have observed that almost every company is talking about the potential technology has for their operations, whether it is transformational innovation in the form of entirely new business models or incremental and sustained innovation through the adoption of new technologies like cloud computing.

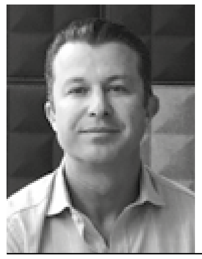
With this increased focus on digital transformation, we have also noticed a marked shift in the demands and expectations of the legal community. Now more than ever, organisations are looking to us, their lawyers, to play a more active role in helping them make key innovation decisions, and advise them on how they can take these steps without compromising on the underlying legal, regulatory or compliance fundamentals of their businesses. This is no easy task.

That said, attitudes and practices within the legal community have also changed. There has been a noticeable increase in the appetite of lawyers to become the agents of change, and move away from some of the stereotypical risk-averse behaviours that lawyers traditionally exhibited. Although the digital transformation journey does present challenges to the legal community, in terms of understanding new and emerging technologies and applying traditional legal principles to such technologies, we are overwhelmingly of the view that it presents enormous opportunities for the profession. Digital transformation offers an opportunity for the legal community to become trusted partners as we enable the organizations we advise achieve their digital ambitions.

This paper represents a unique partnership between Microsoft and Linklaters in our shared commitment to support you during your digital transformation journey. For both of our organisations, innovation is at the heart of what we do; in terms of how we do business and how we partner with our customers and clients.

We hope you find “**Lawyers: Agents of Change in a World of Digital Transformation**” a useful resource, and we look forward to continuing the digital transformation conversation with you.

Adrian Fisher
Counsel, TMT
Linklaters



Andrew Cooke
Assistant General Counsel &
Regional Director - Legal Affairs,
Microsoft Asia

A joint publication by Linklaters and Microsoft

Contents

1. Introduction

The world is transforming faster than ever before. Traditional business models across many sectors have either already been disrupted by new and agile players, or are facing imminent disruption. No matter which industry an organisation belongs to, they all share a common focus: the need to contemplate and implement profound strategies of digital transformation.

At its heart, digital transformation is about using technology to enable a business to be more agile and efficient, and to provide better service to its customers.

So, what does this all mean for lawyers?

Digital transformation presents an opportunity for lawyers to influence, to collaborate and to partner with a range of stakeholders to enable the delivery of secure and compliant digital transformation solutions. Lawyers must develop a reputation within their organisations or with their clients for being enablers of change and a collaborative force, rather than being inhibitors of innovation.

This paper presents **three Digital Transformation Practice Principles** designed to equip lawyers (both in-house and in private practice) with the tools and the mindset to become agents of change:

- **Create Clarity.** Lawyers can expect to be presented with a digital transformation solution and be asked by their business stakeholders or clients, *"Can we do this?"*. To be able to answer this question clearly and confidently, the lawyer will first have to upskill and have a deeper understanding of the technology in question. With a clear understanding of what the technology is and what it offers, the lawyer must also be flexible in applying to that technology legal principles that were likely not developed for the digital age. This will help them guide organisations to build a stronger digital solution that it is compliant and secure by design.
- **Build Partnerships.** Digital transformation is often led by senior management. However, lawyers have an opportunity to get a seat at the table from the outset of any digital transformation deal. Often the lawyer is the person who bridges a number of the most important gaps in the digital transformation process – the gap between the business and operations teams and the business and the compliance function; the gap between the company and its regulator; and the gap that often appears in negotiations between a customer and a supplier. Through early engagement, collaboration and partnership with key decision makers, lawyers will move up the value chain and establish themselves as a fundamentally important part of the creative process in any digital transformation project.
- **Deliver Success.** Getting clarity around the technology and collaborating early with stakeholders culminate in a lawyer's principal role – successfully navigating the issues in a digital transformation deal to deliver the best result for the organisation. A lawyer who is equipped to cut through the noise and the buzzwords and clearly identify the key legal and commercial risks for their company or client will ensure they are driving innovation and pursuing the right outcomes by protecting their business's reputation and best interests.

A joint publication by Linklaters and Microsoft

2. A Primer on Digital Transformation

What is Digital Transformation?

Digital transformation is about using technology (like cloud computing) to enable a business to be more agile and efficient, and to provide a better service to its customers.

Digital transformation will take different forms for different companies. When we think about digital transformation, we often think of a fundamental shift in how we do things – the complete replacement of manual practices with digital or automated processes. This is not always the way digital transformation will work, and for many organisations there is benefit from implementing incremental changes (for example, digitising certain practices) rather than transforming an entire business model.

The forms that digital transformation deals can take can be viewed in a spectrum:

"Quick wins"	Solution-centric engagements across business lines / industries	Transformational deals
At one end of the spectrum, digital transformation deals comprise targeted, strategic steps to improve operational or organisational processes, and serve as "quick wins" for an organisation. These types of deals typically form the foundation for digital transformation of a business. For example, these could involve introducing a digital customer experience by developing a customer-facing mobile application. For a lawyer, this type of deal may not look much different to a standard software procurement that they are used to negotiating but different issues may arise (e.g. big data analytics, or the incorporation of artificial intelligence) and the lawyer should, again, be able to anticipate those legal issues before they arise.	In the middle of the spectrum, digital transformation could take the form of organisations wanting to implement industry level solutions, such as data analytics to understand the industry's customer insights and solve particular business problems. Organisations may also want to roll out solutions that cover a range of business lines, such as a shift to digital marketing. The key for a lawyer in these deals is to go deep in learning about the legal, regulatory and policy issues specific to the industry and to become a true subject matter expert in the fundamentals and nuances of those issues.	And at the other end of the spectrum, digital transformation deals can involve a complete reimagination of a business, or even the rolling out of new commercial and revenue models, requiring a comprehensive roadmap for change over a short to medium term. Some examples of this are the resources company that no longer has people physically located at mining sites or the bank that is truly digital-first. Due to their complexity, from a legal perspective, these deals will be the most challenging and provide the most opportunity for a lawyer to take a lead role in scoping the deal and ensuring risk is properly assessed and managed.

The common thread that ties this spectrum of digital transformation deals together is that the organisations themselves may be less focused on the digital products or technology to be adopted and implemented, but more holistically on the **business solutions and outcomes** they can deliver using those products and technology. The lawyer, however, will need to know and understand the technology that underpins the transformation in order to provide considered advice and be assured of the compliant nature of what is being undertaken.

What drives Digital Transformation?

It starts with the customer.

Customers' profiles are changing, and so are their demands and how they expect to interact with businesses. Building a *relationship* with the customer is so much more important now than ever before, as customers can often switch between businesses as easily as tapping on an alternate application. Businesses (especially the incumbents and those operating on traditional models) need to acknowledge this or face the looming threat of either their products becoming obsolete, or being out manoeuvred by their more agile and efficient competitors. Given the current hyper-competitive business landscape, where it used to be a risk to do something new, it is now a risk to not do something new or different.

To generate new sources of revenue and to stay relevant, companies are seeking to reimagine the customer journey and experience. As they reinvent how to connect and engage with their customers in new and exciting ways, an organisation will also need to ensure that its operational and organisational processes internally are likewise empowered to support and effect that change. Empowering employees will help drive optimised operations and processes, and in turn lead companies to transform their products and services.

We have identified four core drivers that business stakeholders think about when considering digital transformation:

1. Engaging Customers – Giving them new experiences they love

With the rise of mobile and social technologies, customers are now more powerful than ever. Their always-connected status and ability to find information in seconds puts them in control of their own experience, and this trend has forced businesses of all sizes to rethink how they engage and connect with their customers. Customer engagement starts by understanding customer behaviour. Intelligence plays a critical role in understanding and dissecting massive amounts of data to recognise patterns of sentiment and behaviour across a customer base.

2. Empowering Employees – Reinventing productivity and enabling a data-driven culture

Organisations cannot transform to digital unless people do. The nature of how employees work has undergone a dramatic evolution. Successful businesses use the power of mobility to support employee productivity and collaboration, while mitigating the risks that come with providing freedom and space to employees.

3. Optimising Operations – Modernising the portfolio, transforming processes and skills

Operationally, organisations will also need to accelerate the responsiveness of their business, improve service levels, and reduce costs with intelligent processes that anticipate the future and coordinate people and assets more efficiently.

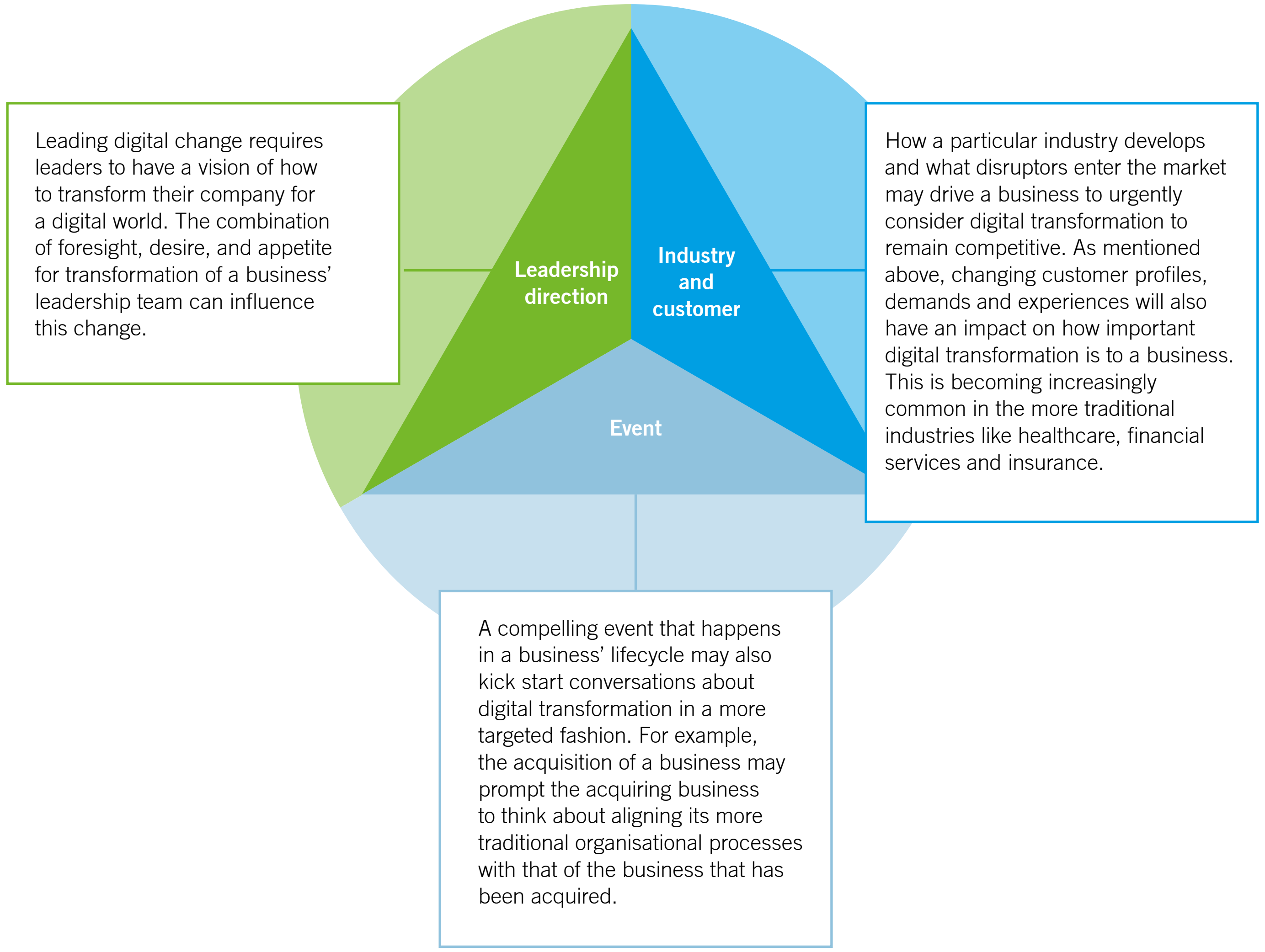
4. Transforming Products – Innovating products and business models

Leveraging data as a strategic asset, organisations can shift from hindsight to foresight, automate manual processes, deliver personalisation to customers, and innovate with new business models, services, products and experiences, all to differentiate and capture emerging revenue opportunities.

Businesses will also implement digital transformation at different times and pace.

While some are looking to build digital capabilities, others might be looking to build digital businesses. Much will also depend on the level of technological maturity and sophistication of a business and the industry in which it operates.

The main pivots which may prompt a digital transformation of a business can take varied forms but are often triggered by one of the following:



Leading digital change requires leaders to have a vision of how to transform their company for a digital world. The combination of foresight, desire, and appetite for transformation of a business' leadership team can influence this change.

How a particular industry develops and what disruptors enter the market may drive a business to urgently consider digital transformation to remain competitive. As mentioned above, changing customer profiles, demands and experiences will also have an impact on how important digital transformation is to a business. This is becoming increasingly common in the more traditional industries like healthcare, financial services and insurance.

A compelling event that happens in a business' lifecycle may also kick start conversations about digital transformation in a more targeted fashion. For example, the acquisition of a business may prompt the acquiring business to think about aligning its more traditional organisational processes with that of the business that has been acquired.

Digital transformation can also happen in a series of micro revolutions. It may initially start with small and targeted digital solutions, but as the organisation grows in digital maturity, it may eventually undergo a full and fundamental digital transformation.

3. Digital Transformation Practice Principle 1: **Create Clarity**

So how can lawyers respond when they are presented with a digital transformation solution and are asked by their business stakeholders or clients, **"Can we do this?"**?

Our first Digital Transformation Practice Principle is to **Create Clarity**. The ability to create clarity manifests itself in two ways: (a) understanding the technology used in the digital transformation deal; and (b) applying existing legal principles to that technology.

Firstly: Create clarity by understanding the technology. A fundamental requirement to be an effective lawyer in digital transformation deals is to first have a clear understanding about the new technologies presented to them. A healthy dose of curiosity is needed, and lawyers must embrace flexibility and adaptability to understand these new technologies to apply legal principles properly to them.

For example, organisations are starting to think about use cases for technology such as blockchain, artificial intelligence, chatbots, and cryptocurrency. If presented with this challenge, how many of us can say that we understand these technologies deeply enough to be able to meaningfully approach the legal issues relating to them?

Lawyers should not be fearful that they lack the skills to support digital transformation projects simply because they do not have an intimate understanding of the technology being used. The key is making sure you are armed with the knowledge to de-mystify the technology, which for many lawyers will require a mindset change, an openness to learn, and access to those who can provide the right technology training. At Linklaters, we have found that a key role that organisations look to external counsel for as part of their digital transformation is helping in-house lawyers to re-skill by partnering on training not only in new areas of the law but also in industry trends and technology.

Secondly: Create clarity by applying existing legal principles to that technology. What lawyers often find when looking at digital transformation deals is that the fundamental legal issues associated with these deals are generally not new ones simply by virtue of the fact that the organisation is digitising its business. These issues have existed, and will continue to exist, no matter how the organisation functions (whether in a more traditional model or digitally).

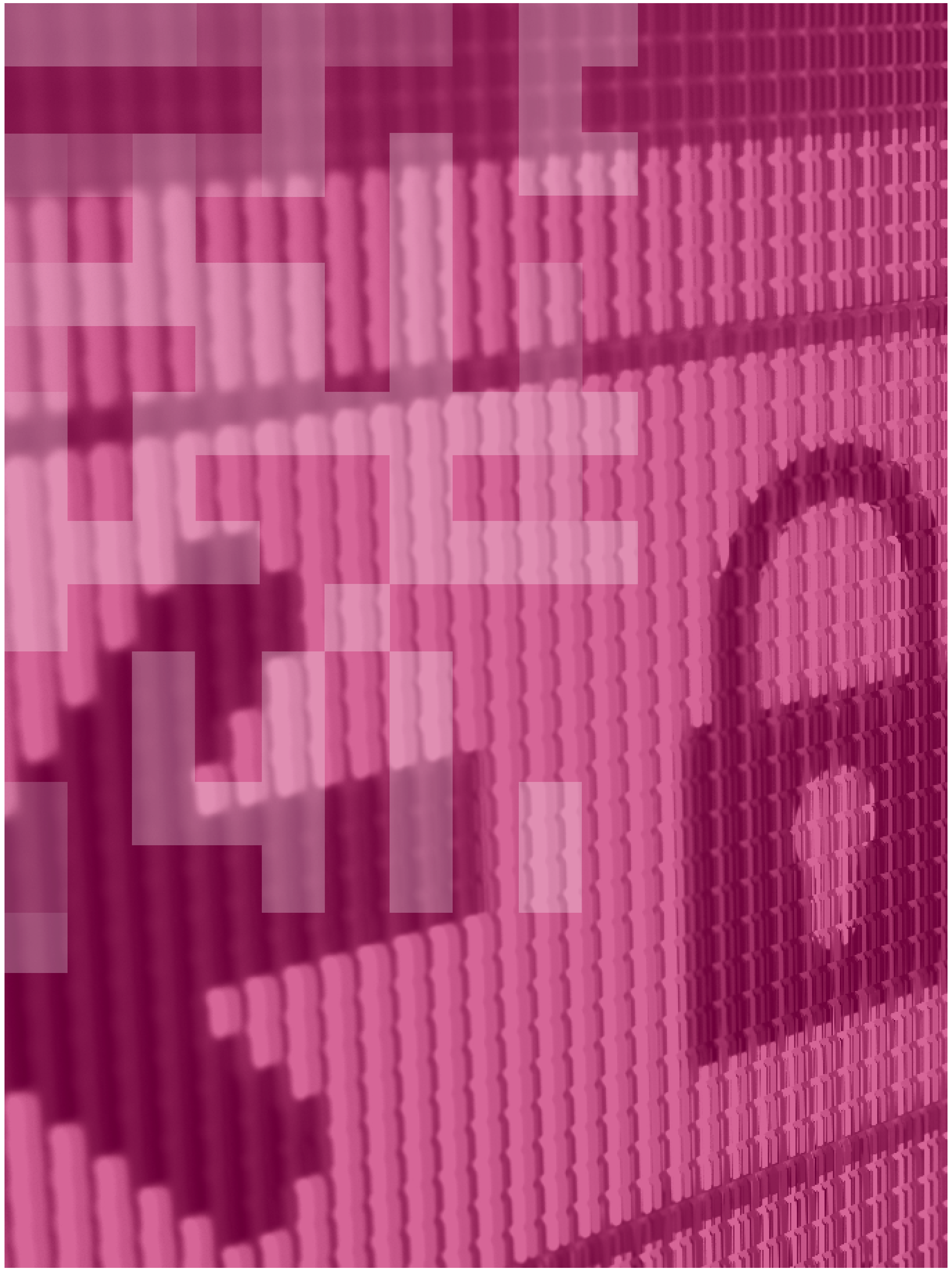
For example, companies that are supervised by regulators (like banks, insurers and telecommunication companies) will continue to be regulated and often the regulation, although it has not evolved to deal with digital issues, is principles-based and technology agnostic. Similarly, the laws on intellectual property, data privacy and consumer protection are all technology neutral and so the same legal principles will apply (albeit in a slightly different way) whether you are using a traditional on-premise solution or a more agile cloud solution.

This should give some comfort that digital transformation deals do not necessarily present an inordinate amount of added risk, at least from a legal and regulatory perspective.

As an example, data privacy regulation will exist whether or not a business operates in analogue or digitally. However, digitising the business will raise important issues around, for example:

- cross-border transfer of data, particularly as cloud will be at the core of most digital transformation;
- whether you may lawfully use customer personal data for a new set of purposes which the digitising of a business might bring, such as big data analytics or direct marketing; and
- whether any new IT architecture that is rolled out as part of the digital transformation process has sufficient technical and security arrangements to protect the data in accordance with regulatory expectations.

Some of these issues, such as the one on IT architecture above, will inevitably involve complex technical discussions, reinforcing the need for lawyers to collaborate closely with other stakeholders such as the IT and security experts to get comfortable that the technology matches the regulatory and compliance requirements that the business needs to comply with. Without forming this partnership with the technical team, it would be very easy for the legal team to err on the side of caution, and therefore assume the role of a blocker, and not an enabler.



4. Digital Transformation Practice Principle 2: **Build Partnerships**

Henry Ford once said, “If everyone is moving forward together, then success takes care of itself”. We cannot emphasise enough how important it is for lawyers to focus on early engagement and to collaborate and build partnerships with their business stakeholders and key decision makers.

Digital transformation is often not an easy process or an off-the-shelf solution. It requires organisations to reflect deeply on their strengths and weaknesses, their capability and resources, their vision and strategy. This cannot be done in isolation. As discussed, there are varying catalysts for digital transformation and digital initiatives may take various forms. This highlights that, for a lawyer, early engagement with the business and management and ongoing collaboration with the other stakeholders during the process is critical so that the legal team is informed and ready to advise clearly and execute digital transformation deals smoothly and successfully.

Legal teams can work as enablers or inhibitors of innovation. A conservative or cautious leadership team may shy away from digital transformation prematurely if its legal team responds negatively to a proposed transformation process. In contrast, an effective legal team may be one that does not simply say “no” when they identify issues and risks, but instead offers alternative ways forward and undertakes a considered analysis in partnership with the leadership team to develop a shared understanding and co-create an effective course of action. This type of collaboration by a considered and pragmatic legal team would certainly demonstrate highly-valued partnerships.

In our experience, organisations that have most effectively implemented digital transformation projects have been those who present a seamless team of internal stakeholders (ranging from commercial, IT, security, legal, compliance) each of whom know intricately both the business and its objectives and risk appetite, and the roles and responsibilities of each of the other stakeholders. These organisations are able to work nimbly and deal with challenges with adaptability because they share the responsibility and ownership for the project amongst these different stakeholders. Organisations who work in a siloed fashion where, for example, lawyers are not encouraged or enabled to be part of the overall deal team are more likely to face delays in executing contracts or face hurdles at the last minute when new issues arise.

To ensure that legal teams play this facilitative role, they can do the following:

- ✓ Understand the leadership team’s innovation agenda, its objectives for the transformation, and what technology underlies that transformation to facilitate a move in that direction. To do so, the legal teams need to be involved in the conversation from the beginning.
- ✓ Engage in “Compliance by Design”, an approach to digital transformation which considers legal and regulatory compliance throughout the whole transformation process. This will mitigate against a situation where the legal team is engaged in the conversation when the transformation process is more mature, only to have the unenviable task of raising all the potential issues with the leadership team at a late stage.
- ✓ Map out the customer journey so that they can identify and resolve the potential legal issues and pain points throughout that journey in the most agile way.

To that end, partnership with the relevant stakeholders in the leadership, business and technical teams is vital. The legal teams must develop a reputation within their organisation for being enablers of innovation and a collaborative force.

5. Digital Transformation Practice Principle 3: **Deliver Success**

You have understood the technology to be implemented. You have also engaged early with the business stakeholders and key decision makers to better understand what the organisation's digital transformation objectives and solutions are. You have mapped out the customer journey, and have flagged potential legal issues and pain points.

This has set you up nicely to execute one of the principal roles you will play in any digital transformation deal – successfully navigating the issues in a digital transformation deal to deliver the best result for your organisation.

In a survey conducted by IDC[1] across 18 countries to assess the attitudes of key decision makers towards innovation, in-house risk teams and in-house lawyers were identified as more influential on a business' cloud deployment decisions, even over in-house IT staff and outside IT consultants. This data tells us that lawyers are pivotal to the success or failure of new ventures (more so than we would imagine!), and so it is about making sure that you and your legal team position yourselves to drive success in your organisation.

For lawyers who have not dealt with digital transformation deals before, this may be a daunting task as it often involves having a deep understanding across a broad range of issues such as data protection, intellectual property, contracting structures, and exit and transition management. Lawyers will need to upskill themselves on technology, and collaborate with the right subject matter experts to better engage in a meaningful assessment of the key legal and commercial risks involved in a digital transformation project. This process should not be approached in a siloed fashion. Digital Transformation Practice Principles 1 and 2 continue to be an integral part of the journey. Having clarity around the technology in question and constant collaboration with various stakeholders is key.

Then there is something to be said about the negotiation process itself. What legal teams might find in the course of a digital transformation deal is that no matter how greatly prepared they are before they reach the negotiation table, deal processes can dramatically slow down or fall over because of poor deal discipline. In order to ensure that all your legal team's preparation and efforts are not lost when the time for negotiations comes, some thought will need to be given to ensuring deal discipline throughout this process. This will include:

☑ Having good project management and securing the availability of the right stakeholders for the appropriate meetings who can make business decisions relevant to the issues to be discussed.

☑ Setting agendas before negotiation meetings so that everyone at the table is on the same page about the objectives to be achieved at those meetings.

☑ Having discipline to focus the negotiations on the issues that are important to your organisation.

To give you a head start in this journey, we have put together in the next section some key "tools of the trade" that will empower you to successfully close digital transformation deals. We also highlight some key legal, regulatory and commercial issues that you should be mindful of when approaching digital transformation deals. We hope that these will empower you to be agents of change and to deliver success to your organisations and clients.

[1] IDC, "Advising to Innovate – views from the Asia-Pacific Legal, Risk and Compliance Communities", April 2017.

Skilling up to be Agents of Change

In designing this section, we have identified some of the key legal touchpoints that permeate through most digital transformation deals. This is not meant to give you an exhaustive list of items to consider, but our hope is that this will be the first step in your journey to becoming an effective digital transformation lawyer.

This section is divided into two parts:

- **Part 1**, contributed by Linklaters, explores key legal and commercial issues which often surface and which lawyers should be mindful of when approaching digital transformation deals.
- **Part 2** is a dedicated section on cloud, the technology on which digital transformation is built. It explores what cloud technology is, and provides nine best practice principles that Microsoft Asia has developed that lawyers should carefully consider when an organisation looks to implement a digital transformation project, powered by cloud.

Part 1: Key Legal and Commercial Issues in Digital Transformation Deals

Every digital transformation deal will be unique in some way, and undoubtedly present different legal issues. We set out below a list of some of the key legal and commercial issues that most often arise in digital transformation deals to give you a flavour of what to expect.

1. Define the scope of what is being provided.

Digital transformation can be an amorphous expression, and you may find yourself being fed broad instructions (like 'we're replacing function X with a cloud-based machine learning and analytics platform') that do not clearly identify what is actually being provided. It is important at an early stage to clearly identify what products and services comprise the digital transformation solution. For example, is your business procuring a platform on which it can build its desired functionality? Or will some type of software-as-a-service offering be provided where that functionality is provided effectively as a managed service? The answer to this question will bring clarity regarding not only legal issues around the terms of use by that organisation, but also the technical issues around security of data and what support services are required by the organisation to maintain the system. It will also be important to consider what ancillary transaction documents will comprise the suite of documents to be signed for the deal.

2. Contracting models.

Consider what the commercial arrangements in the deal might look like. They could be with multiple parties such as systems integrators, cloud providers, developers and even data scientists. Or, they could be with a single partner who will have primary responsibility for creating and delivering a digital solution. In more targeted digital transformation deals where discrete processes are being digitised, the contracting models may still look like they would in a standard licencing transaction. However, the larger, more transformational deals are likely to move away from standard licensing models to more bespoke, holistic, full product and service packages which may include system customisation and integration services, consultancy services, and support and maintenance services.

3. Triggering outsourcing requirements.

These new contracting models may raise new regulatory issues which lawyers must consider. Consider whether or not the digital transformation contracting structure looks more like a bespoke outsourcing-type arrangement, as opposed to a simple in-license of technology. Outsourcing arrangements may trigger regulatory requirements (such as notification or approval requirements) in the more regulated industries like the financial services sector. There may also be industry-led technology risk management guidelines or practices that need to be considered.

4. Waterfall v agile contracting.

Traditional outsourcing and development arrangements rely heavily on strict processes being followed with completion of one step (e.g. developing of design specifications) leading to the next (e.g. commencement of development work in accordance with those specifications). Agile contracting (which encourages flexibility in how a product is designed and delivered) may be appropriate to allow for pivots in the process and to track the success of the different stages of implementation. However, agile contracting can sometimes blur the lines in terms of the responsibilities of the parties, and so it is critical for the roles and responsibilities of the parties in the course of the arrangement to be clarified so that the project progresses as efficiently as possible. There is also often a higher risk for the customer with agile contracting methods as there is less certainty compared to traditional contracting models. This risk can be mitigated by ensuring that there are good governance controls in place (e.g. monthly project management meetings) so that parties have visibility over the progress of the project.

5. Intellectual property management.

Digital transformation deals may involve complex systems integration, and sometimes organisations may want a variety of third-party systems integrated into one platform. As such, parties to a digital transformation deal may have to get comfortable moving away from a very binary "I own this, you own that" discussion around intellectual property rights. For example, if an organisation requires a particular third-party software to be provided on the main service provider's platform, the organisation may have to get comfortable that it will not be able to own all third-party software, even if the main service provider provides some level of customisation to that software at the customer's request. Another tension might be around whether the service provider can own any intellectual property (such as algorithms or code) that it develops for the customer, but which it may need to re-use in some form for its other customers as well. Often obtaining robust rights to use IP can be as effective as securing ownership. If the deal gives rise to patent rights, then the management of the intellectual property portfolio for the project will be much more involved. Parties should be careful that the invention is not released to form part of the state of the art (and hence lose its novelty), and so the necessary confidentiality obligations should be put in place to ensure that does not happen.

6. Data management.

Data tends to be at the heart of many digital transformation deals. With the introduction of augmented intelligence and machine learning functionality, large amounts of data generally need to be used to 'teach the machine' and to build up useful algorithms. While data itself may stay with the organisation, the service provider may need to have residual rights to use the learnings from that data. Organisations must first consider their own regulatory requirements around sharing that data with service providers – for example, does it have the right consents to do so? Separately, organisations should also be concerned with security or applicable regulatory requirements which they may want to impose contractually on the service providers. In this respect, service providers must think about how they can help their customers comply with their regulatory requirements. Things can also get quite complicated where both parties contribute data to a project – in that case, if new data output is generated from the analysis of both parties' data, parties will need to decide how each party can use that output moving forward, and which party will own that output.

7. Pricing.

Digital transformation deals are likely to be priced differently from simple technology licensing arrangements. Instead of traditional licensing fees and prices per user or seat, digital transformation deals may involve pricing based on milestones in the development phase, or on a price-per-use model in the implementation phase. For example, if a car manufacturer is looking to partner with a technology company to design and build AI-powered smart cars for the future, the technology company may consider charging a base service fee for the development phase to cover its research and development costs, but look to charge a fee based on a per-unit basis for cars that have been successfully built or sold during the manufacturing and go-to-market phase.

8. Termination and exit.

Because digital transformation deals will often involve complex integration of systems, these deals may be difficult to unwind or terminate. As such, it can be expected that termination provisions in such deals are likewise complex, contemplating processes such as exit management plans, governance models involving key executives, and consideration given to transferring systems to an alternate service provider. Termination for convenience provisions for the organisation are a nice-to-have, but are less common in large digital transformation projects as both parties are equally invested in building a successful solution. Organisations should therefore ensure that they have considered all the various permutations of when it may need to exit the deal, and consider the processes around how that exit will happen and over how long.

9. Risk and liability.

As every digital transformation deal will be different, how risk and liability is allocated between the parties may also differ from more traditional arrangements. Key to this issue will be an open discussion between service providers and customers on what risks they face as part of the project and how they should and can be protected against those risks. Some risks will be unique to the organisation and its particular industry, and so another important consideration is to ensure that the organisation is fully aware of what regulatory requirements it is subject to, and what impact they have on the digital transformation deal.

Part 2: De-mystifying the Cloud, and Microsoft's Safe Cloud Principles

Digital transformation is more often than not powered by cloud. As such, a working understanding of cloud technology is fundamentally important for any lawyer advising on a digital transformation deal. This section provides a brief introduction to cloud, and explores Microsoft's Safe Cloud Principles, which reflect many years of conversations that Microsoft has had with customers, regulators, industry associations and the legal community.

What is Cloud?

Cloud computing or cloud services means on demand network access to a shared pool of configurable computing resources. In other words, cloud services provide organisations with on-demand access, using a network connection, to information technology or software services, all of which a cloud service provider can configure to the needs of the customer.

Service Models

There are three common delivery models for cloud services:

- **Infrastructure as a Service (IaaS)**, where the cloud service provider delivers IT infrastructure e.g. storage space or computing power.
- **Platform as a Service (PaaS)**, where the cloud service provider provides a computing platform for customers to develop and run their own applications.
- **Software as a Service (SaaS)**, where the cloud service provider makes available software applications to customers over a cloud service.

Deployment Models

There are four common deployment models for cloud services, each characterised according to: (i) who manages the day-to-day governance, operation, security and compliance of the service; (ii) who owns the infrastructure (including physical infrastructure such as facilities, computers, networks and storage equipment); (iii) where the infrastructure is located; and (iv) who can access the data being hosted. They are:

- **Private Cloud**, with infrastructure being owned and managed sometimes by the customer, but more often by the cloud service provider. The infrastructure is located either on the customer's premises or, again more typically, on the cloud service provider's premises. In all cases, the data and services are accessible exclusively by the particular customer.
- **Public Cloud**, with infrastructure being owned and managed by the cloud service provider and is located off-premise from the customer. Although the data and services are protected from unauthorised access, the infrastructure is provided to a variety of customers. Public Cloud is also referred to as a 'multi-tenanted solution' because there are multiple customers who will be provisions from to the same infrastructure.
- **Community Cloud**, which serves members of a community of customers with similar computing needs or requirements, such as security, reliability and resiliency. The infrastructure may be owned and managed by members of the community or by the cloud service provider. The infrastructure is located either on the customer's premises or the cloud service provider's premises. The data and services are accessible only by the community of customers. Community Cloud is by its nature a 'multi-tenanted solution' because there are multiple members of a community of customers who will all have access to the same infrastructure.
- **Hybrid Cloud**, which is a combination of two or more of a Private Cloud, Public Cloud or Community Cloud. Hybrid Cloud infrastructure can be owned and managed by the customer, or by the cloud service provider and in either case the infrastructure may be located on-premise or off-premise, or both (e.g. some on-premise Private Clouds integrate with off-premise Community Cloud or Public Cloud). The data and services can be accessed based on the design of the solution, corresponding to whether the architecture has public, private or community characteristics. Hybrid Cloud may be a 'multi-tenanted solution', if multiple customers have access to the same infrastructure. It can however also provide a 'dedicated' solution or component.

Microsoft's Safe Cloud Principles

Through its conversations with customers, partners, regulators and industry bodies, Microsoft has developed a set of Safe Cloud Principles. These Principles are a unified, condensed and clarified set out of best practices to help organisations (and in particular, lawyers) to focus on and navigate through the relevant regulatory and legal issues when contemplating a move to the cloud. Microsoft is sharing these Safe Cloud Principles in the interests of advancing the digital transformation conversation and sharing what they have learned through the discussion process.

The Safe Cloud Principles are:

1. Service provider reputation and competence

Organisations should carry out, and cloud service providers must assist in facilitating, a risk assessment and due diligence on the cloud service provider to ensure that the cloud service provider and its cloud services meet the legal, regulatory, contractual and business requirements. Organisations should also have in place a risk management plan that includes measures to address the risks associated with the use of cloud services.

As part of the due diligence process, organisations should ensure that they understand the pros and cons of each of the cloud service deployment models and the specific configuration being proposed by the cloud service provider to determine whether it is suitable for the organisation's purposes and can meet its regulatory requirements.

Some industries make this due diligence and risk management process mandatory. For example, most financial regulators require financial institutions to carry out impact assessments prior to entering into the contract for cloud services.

2. Review, monitoring and control

Legal and regulatory compliance does not end when the digital transformation contract is signed. Cloud service providers should be required to provide regular reporting and information to demonstrate continued compliance with the legal, regulatory, contractual and business requirements throughout the duration of the digital transformation deal. Customers and cloud service providers must meet regularly to review the reports and performance levels. The digital transformation contract should provide for an effective mechanism for remedial actions arising from any issues that emerge or non-compliance.

Cloud service providers should regularly (e.g. annually) provide customers with copies of independent third-party audit results that the cloud service provider has obtained, e.g. SSAE 16 SOC1 (Type II) reports. Cloud service providers should also provide copies of reports of penetration testing that the cloud service provider has carried out or arranged to be carried out by independent third parties.

3. Confidentiality and certified security standards

Cloud service providers must be certified to have and maintain robust security measures and comprehensive security policies that meet or exceed international standards (ISO27001 and ISO27018 accreditation should be a minimum). Customers should confirm that cloud service providers use encryption technology that meets or exceeds international standards to protect and secure the customer's data at all times.

Certification is an important benchmark to measure security standards. There is currently no one recognised industry certification specifically for cloud services. However, ISO27001 and ISO27018 are generally considered the most appropriate certification given the high benchmark that cloud service providers must meet to achieve and maintain them. Other cloud service provider certifications can also be indicative of industry best practice and should also be taken into consideration (e.g. if the cloud service provider has been granted authority under FISMA (the US Federal Information Security Management Act) or is HIPAA compliant).

In many countries, maintaining confidentiality is also a legal requirement imposed by statute and/or by case law and again, certification (like ISO 27018) is a useful tool to meet this. Privacy regulations also often require organisations to maintain high levels of security in respect of personal data in order to ensure that the privacy of individuals is safeguarded, and personal data does not get into the wrong hands.

4. Resilience and business continuity

The cloud service must be reliable. Cloud service providers must have an effective business continuity plan with appropriate service availability, recovery and resumption objectives and with regularly tested and updated procedures and systems in place to meet those objectives. The risks of downtime should be minimised through good planning and a high degree of system resilience.

This is an important principle as service disruption can have significant impact on the customer and its industry. While it should be recognised that service disruptions can happen, the risk of them arising and their effect can be minimised through having in place appropriate business continuity plans and procedures. Customers must ensure such plans and procedures are in place and regularly tested and updated, to help protect against service disruption.

5. Data location and transparency

Cloud service providers must disclose where data will be located. Customers should ensure that the government policies, economic and legal conditions of the identified locations are safe, stable and appropriate.

Regulators (e.g. financial regulators or privacy regulators) typically require that organisations at all times know the location from where a cloud service provider will process their data. A cloud service provider's data centres must be located in safe, stable and secure places, where confidentiality and privacy obligations are observed, upheld and enforced by the local legal system.

6. Limits on data use

Cloud service providers should not use customers' data for any purpose other than that which is necessary to provide the cloud service. The contract should prevent cloud service providers from using data for any secondary purpose (e.g. marketing and advertising). This also helps to uphold the confidentiality of the customer's data and prevent it from being misused or disclosed (Safe Cloud Principle 3).

Privacy regulations also typically require that organisations must not allow personal data to be used for any purposes beyond the purpose for which the personal data was collected. This protects individuals' privacy so that their personal data is only used for the purpose that the individual would expect.

7. Data segregation and isolation

Customers should also expect that their data be segregated (including by way of logical segregation) from other data held by the cloud service provider.

Requiring cloud service providers to ensure that a customer's data is segregated from other data will ensure the security and confidentiality of the customer's data is maintained (Safe Cloud Principle 3) as the integrity of the data is preserved. Data segregation will also help make any termination easier to deal with since all of the customer's data can be more easily returned and deleted (Safe Cloud Principle 9).

As noted above, Public Cloud and Community Cloud are multi-tenanted models. This means that multiple customers will be provisioned from shared infrastructure. Multi-tenanted Cloud Services can still comply with Safe Cloud Principle 7 where the cloud service provider has the ability to demonstrate that through logical segregation, they are able to provide the services in a highly secure manner, so that data storage and processing for each tenant is separated from that of other tenants.

8. Conditions on subcontracting

Limits should be placed on cloud service providers' ability to use subcontractors – they should only be allowed to use subcontractors if the subcontractors are subject to equivalent controls as the cloud service provider.

Most cloud service providers rely on the use of subcontractors to provide certain support services. This should not be a problem, but customers may require that subcontractors are not used unless the cloud service provider ensures that the subcontractor will have equivalent protections and controls in place as the cloud service provider.

9. Conditions on termination

Customers should have appropriate exit provisions in the digital transformation contract. On termination of the cloud service contract, the cloud service provider should be required to work with the customer to return the customer's data to the customer and then be required to permanently delete the data from the cloud service provider's systems. Any data that does not need to be returned to the customer should be permanently deleted by the cloud service provider.

This requirement also helps maintain and safeguard the confidentiality of the customer's data (Safe Cloud Principle 3). Privacy regulations in most countries also require that personal data is deleted or destroyed when it is no longer required. This requirement protects individuals' privacy so that their personal data will not be held for longer than is necessary by the cloud service provider.

6. Concluding with a Checklist

The world is changing, and the role of legal teams is changing along with it.

Lawyers have a critical role to play in the digital transformation process. As organisations contemplate and implement profound strategies of digital transformation, the legal function has a greater than ever opportunity to collaborate and partner with the leadership team and other stakeholders to cultivate and cement their role and reputation in the business as an enabler, and not an obstacle, to their business' strategies. Part of the opportunity for the lawyer in a digital transformation deal will be:

- **To create clarity** by understanding the technology in question and being adaptable, flexible and equipped to understand the objectives of a digital transformation deal and help create a course of action to achieve them;
- **To build partnerships** by focusing on collaboration and engaging early with the internal and external stakeholders driving the digital transformation deal; and
- **To deliver success** by confidently and clearly identifying the risks involved in a deal and finding solutions to overcome them and successfully close these deals.

If lawyers answer that call to action within their organisations or with their clients, they will create the opportunity to guide their business to achieve its digital agenda as effectively as possible, while not compromising on compliance and security.

We have summarised the points presented in this paper in a simple checklist for you to consider when approaching a digital transformation deal for your organisation or your client. We trust that this paper has de-mystified digital transformation as a concept, and has equipped you to being well on your way to being an enabler of innovation.

Checklist

Creating clarity.

☑ Do you understand the technology that is being implemented? If not, upskill by checking in with stakeholders in your organisation or client (e.g. the IT teams) that can help you do so.

☑ Have you put on your "Compliance by Design" hat? Be ready to be agile in your problem solving, and also be creative in doing so.

Building partnerships.

☑ Have you engaged the business stakeholders and key decision makers early in this process?

☑ Do you understand the leadership team's digital transformation agenda (i.e. what its objectives are, what the drivers are, when they want the solution to be implemented)?

☑ Have you mapped out the customer journey to predict where the pain point legal and regulatory issues might arise?

☑ Are you clear on the roles and responsibilities of the deal team to ensure that deal discipline is maintained, and the project progresses smoothly and efficiently?

Delivering success.

☑ If the digital transformation deal involves a cloud solution element, have you ascertained what service models and deployment models will be used?

☑ Have you considered the Safe Cloud Principles when negotiating the cloud service arrangement?

☑ Have you listed the relevant legal, regulatory and commercial issues that are most likely to arise in the course of the deal? Have you applied a solution-oriented mindset to how to overcome these issues for your organisation or client?