Navigating your digital transformation journey

A guide for legal & compliance professionals in energy and natural resources companies in Asia-Pacific
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>4</td>
</tr>
<tr>
<td>Part 1: Using technology to transform the energy &amp; resources sector</td>
<td>6</td>
</tr>
<tr>
<td>1. Optimizing operations with real-time, actionable data</td>
<td>8</td>
</tr>
<tr>
<td>2. Empowering a mobile work force</td>
<td>9</td>
</tr>
<tr>
<td>3. Protecting people and the environment</td>
<td>10</td>
</tr>
<tr>
<td>Part 2: Digital transformation: overcoming regulatory and risk management barriers</td>
<td>12</td>
</tr>
<tr>
<td>1. Data Sovereignty</td>
<td>14</td>
</tr>
<tr>
<td>2. Data Security and Privacy</td>
<td>18</td>
</tr>
<tr>
<td>3. Business Continuity</td>
<td>20</td>
</tr>
<tr>
<td>Part 3: Legal and compliance professionals as drivers for digital transformation</td>
<td>22</td>
</tr>
<tr>
<td>1. The changing roles of legal and compliance professionals</td>
<td>24</td>
</tr>
<tr>
<td>2. Delivering a competitive advantage</td>
<td>25</td>
</tr>
<tr>
<td>3. In conversation with Alex Westmoreland</td>
<td>26</td>
</tr>
<tr>
<td>Conclusions</td>
<td>27</td>
</tr>
</tbody>
</table>
Foreword

The energy and natural resources (E&R) sector in Asia-Pacific is undergoing rapid and unprecedented change, driven by macroeconomic trends such as global pressures on commodities prices, a need to find and exploit new supplies and the demands of a changing professional workforce. At the same time, the sector is undergoing a digital transformation, as innovations in new technologies offer powerful tools that can revolutionize how organizations operate. The impetus for change is therefore stronger than ever before. With the fast-changing tides, E&R companies across Asia-Pacific must reassess their strategies to put technology at the core of their businesses in order to stay relevant and competitive.

Powering digital transformation in the E&R sector is cloud technology. E&R companies are partnering with cloud services providers (CSPs) such as Microsoft to empower their organizations to achieve more. However, despite the transformative opportunities presented by the digital revolution, E&R companies in Asia-Pacific have historically been slow in adopting these new technologies compared to organizations in other highly-regulated sectors, like banks or even healthcare organizations. Many E&R companies are hesitant to adopt new technologies because of regulatory and risk management concerns. While important, E&R companies must recognize that these barriers are not insurmountable. Indeed, major E&R companies have already successfully adopted new technologies with many others following suit.

Here at Microsoft, we have witnessed first-hand how new technologies such as the internet of things (IoT) and big data analytics have revolutionized E&R companies’ operations. We also understand the unique challenges of procuring new technologies in regulated industries, having partnered with E&R companies around the world, as well as customers in other highly-regulated industries such as financial services, education and healthcare. Through our experience, we recognize the important role played by the E&R company’s legal and compliance team in the procurement process. Often times acting as gatekeepers, the legal and compliance team must now recognize their changing roles as enablers instead of blockers. To help with the transition, we engage E&R companies, their legal and compliance team and, if necessary, the relevant regulators and authorities to address challenges faced by E&R companies in the adoption of new technologies and ways to overcome such challenges.
Through many years of collaboration, we have developed a pool of practical resources and in-depth experience to help the legal and compliance teams in E&R companies successfully execute digital transformation projects in a way that meets the highest compliance, risk and security standards. We are delighted to share the full benefit of these experiences in this paper with you.

We first highlight how the digital transformation of the sector offers E&R companies compelling opportunities to maximize operational efficiencies, save costs, enhance safety and sustainability standards, and how Microsoft’s technology can help facilitate the evolution of E&R companies into thriving digital businesses. We will then tackle each of the perceived barriers to digital transformation, focusing in particular on cloud adoption in Asia-Pacific and suggest practical steps that E&R companies can take to overcome these barriers. Finally, we look at the opportunities for legal and compliance professionals to drive the digital transformation of E&R companies.

We hope you find this paper useful and we look forward to hearing your digital transformation success stories.

Scott Hunter  
Regional Business Lead  
Manufacturing & Resources  
Microsoft Asia

Chan Yoon  
Senior Attorney  
Corporate, External & Legal Affairs  
Microsoft Asia
Part 1: Using technology to transform the energy & resources sector

Many E&R companies operate using “tried and tested” processes and legacy technologies that have proven successful thus far. These companies therefore may lack the desire to adopt new technologies. In addition, the lack of familiarity with concepts such as cloud computing, big data or artificial intelligence (AI) may also contribute to the hesitation in embarking on the digital transformation journey.

Increasingly, however, we see more and more E&R companies taking their first steps in adopting new technologies. These forward-looking E&R companies recognize that retaining their competitive edge necessitates a willingness to adopt new technologies. Indeed, many E&R companies in Asia-Pacific have revolutionized the way they operate and have reaped benefits that were previously impossible with existing technologies. In this section, we outline how using new technologies can unlock key opportunities for E&R companies in Asia-Pacific.
1. Optimizing operations with real-time, actionable data

Oilfields, mining locations and drilling platforms generate vast amounts of data. To be actionable, however, the data needs to be readily accessible, real-time and processed via powerful computing systems. When leveraging cloud services, E&R companies have streamlined real-time access to data sets that support predictive and business analytics. Cloud-enabled big data hubs create the opportunity for multi-tier visibility across supplier and customer networks. Such features can be used to optimize production, maintain safety, save costs, and maximize the recovery of reserves by delivering tactical, operational and strategic insights to everyone in the organization based on their job role and decision-making processes. These create a more intelligent, digital E&R company organization.

Case Study: Seadrill

Seadrill is a leading oil and gas deep-water driller, operating globally with a workforce of 6,000 people. Each of Seadrill’s rigs generates huge volumes of data, and the company uses Power BI and Microsoft's Data Warehouse technologies to bring together safety, operations and financial data from various systems and turn these into actionable insights. The use of Microsoft’s technology has enabled Seadrill to assess rig performance and predict failures while at the same time optimize the performance of the rig. In addition, Seadrill is able to see exactly which resources are going into their inventory for planned and corrective maintenance. These insights have been a game changer for Seadrill, allowing the company to reduce costs and unlock significant business advantages.

customers.microsoft.com/en-us/story/seadrill

Case Study: Schneider Electric

Schneider Electric is a global specialist in developing connected technologies for energy management and automation. With connected assets distributed across a country or around the world, edge analytics makes remote asset management easier by putting application logic onsite. However, some businesses may have remote assets without easy access to the cloud, and they may be reluctant to send data outside their own networks. Schneider Electric set out to solve that challenge for the oil and gas industry. The company has pushed edge solutions into new, predictive realms with the help of Azure Machine Learning and Azure IoT Edge.

customers.microsoft.com/en-us/story/schneider-electric-extends-access-to-electricity
2. Empowering a mobile work force

New, agile ways of working are changing the way in which the E&R sector operates. Many E&R companies are investing in technology to enhance the productivity of their workers, especially those who are spread out over a large geographic area, and to manage critical components of the business such as field maintenance, outage response and mobile operations. Forward-looking E&R companies are prioritizing mobility as part of an organization-wide transformation so they can operate on a common data model that facilitates collaboration between workers, partners and even customers around the world. Add cloud computing to the mix and E&R companies have the capability to support maintenance and operational teams over distributed areas, as well as the opportunity to bring new business models to the market quickly.

---

**Case Study: Innogy**

Innogy is a leading energy company with more than 40,000 employees and 23 million customers in 16 countries across Europe. The company introduced Microsoft Office 365 to improve the support provided by the IT department without increasing demands for maintenance or incurring additional expenditure. The move to Office 365 has led to a deep change in corporate culture, with much greater collaboration facilitated by tools such as Yammer, SharePoint and Skype for Business. Employees are also benefiting from much greater working flexibility with the ability to work remotely from any location, and this has made Innogy a preferred employer in the industry.


---

**Case Study: Trimble**

Trimble, a leading solutions provider in the E&R sector, has expanded their mixed-reality product portfolio by adopting Microsoft’s HoloLens. Through the use of Trimble Connect for HoloLens, Trimble has created a mixed-reality solution that is built into the hardhats of firstline workers to increase coordination between multiple stakeholders. By combining models and aligning holographic data, structural, mechanical, and electrical trade partners are now able to achieve greater collaboration and improve the project management process.

[blogs.windows.com/windowsexperience/2018/02/14/mixed-reality-microsoft-february-update/#9f1WLWWyKld6XrVt.97](blogs.windows.com/windowsexperience/2018/02/14/mixed-reality-microsoft-february-update/#9f1WLWWyKld6XrVt.97)
3. Protecting people and the environment

E&R companies are under pressure to maintain a focus on environmental responsibility and employee safety, both under a growing body of regulation and as a matter of expected good industry practice. Meanwhile, with the ongoing pressure on energy and resource prices, operators continue to utilize older assets in an effort to cut costs and maximize efficiency. Without appropriate controls in place, the risk of malfunction or accident is increased.

Investing in big data analytics gives E&R companies the opportunity to better understand the causes of past incidents and formulate action plans to prevent the occurrence of such incidents in future. Indeed, case studies have demonstrated that big data analytics techniques can provide new insight into the root causes of failures of safety-critical equipment. Furthermore, investments in IoT and advanced big data analytics often lead to increased safety and monitoring capabilities so that malfunctions or incidents can even be anticipated by the E&R companies in advance.

Case Study: Laing O’Rourke

Laing O’Rourke is a leading engineering company that provides services for the construction and maintenance of mining and resources infrastructure. The construction business carries inherent risks, especially when teams are working in one of the most remote regions of the world. Operating in the Australian outback, where heatstroke can injure or even kill workers in hours with little warning, Laing O’Rourke designed a smart hardhat to prevent this. The smart hardhat utilizes Microsoft Azure and Power BI to monitor and analyze the temperature and heart rate of the wearer, plus the external temperature and humidity, and emits a warning sound and vibration to alert the wearer if it detects that he or she is at risk of developing heatstroke.


Case Study: Ecolab Inc.

Ecolab is a leading global provider of water, hygiene, and energy technologies and services. The company and Microsoft worked closely together to deliver water management solutions on a much larger scale, and at a much deeper level, than previously possible. The Microsoft Azure platform, including the Azure IoT Suite, is used to accelerate water scarcity solutions for global industries. The information Ecolab collects from 36,000 water systems in more than 100 countries provides actionable intelligence that can be used to benchmark performance and drive continuous improvement.

customers.microsoft.com/en-us/story/ecolabcustomerstory
“We use Power BI and Microsoft’s Data Warehouse technologies to bring together safety, operations and financial data from various systems and turn these into actionable insight. Being able to make the right decisions is truly a competitive edge.”

Kaveh Pourteymour, Vice President and CIO, Seadrill
Part 2: Digital transformation: overcoming regulatory and risk management barriers

Despite the widespread success of new technologies and their related services, the rate of adoption by the E&R sector in Asia-Pacific has generally failed to keep pace with even the most highly regulated sectors, such as financial services, education, healthcare and the public sector. As a result, the opportunity to benefit from digital transformation in the E&R sector in Asia-Pacific, remains a real opportunity.

To a large extent, digital transformation in Asia-Pacific is powered by cloud technologies which hold the promise of driving enormous societal and economic benefits at an unprecedented scale and pace. However, impeding the adoption of cloud are several perceived barriers, including concerns regarding data sovereignty, data security and privacy, and business continuity management. There are practical steps that E&R companies can take to adopt cloud services in a way that meets all applicable regulatory and risk management requirements. Part 2 examines these perceived barriers and suggest practical approaches that legal and compliance teams in E&R companies may take to overcome them.
### Issue 1: Data Sovereignty

Some countries impose regulatory restrictions on the transfer of seismic and drilling data outside of the country. Whilst these regulations do need to be addressed, they may be managed through data classification, stringent cloud service provider (CSP) selection criteria and appropriate regulator engagement.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The common perception is that certain data may only be transferred out of jurisdiction with express regulatory approval. This often presents a barrier to cloud adoption as the core benefits of cloud services are to provide geographical redundancy in data storage and processing which typically requires the flow of data across borders.</td>
</tr>
<tr>
<td></td>
<td>Certain countries in Asia-Pacific (such as Malaysia, Indonesia and Vietnam) do not allow seismic and drilling data to be transferred out of the country without state approval. These restrictions stem from regulations that were put in place decades ago to prevent explorers from leaving the country with valuable hardcopy maps. These restrictions also stem from the fact that, in many countries, seismic and drilling data are regarded as being owned by the state. However, these restrictions only apply to one specific category of data — seismic and drilling data — meaning that all other categories of data remain unrestricted and are only subject to more general confidentiality and data protection laws. These laws typically do not prevent the transfer of data out of jurisdiction. Even where seismic and drilling data are involved, requests for state approval are not necessarily rejected as a matter of course. We are aware of E&amp;R companies gaining approval for the transfer of data to their related off-shore entities through putting in place inter-company agreements to uphold confidentiality of the data. Similar approval has been received by E&amp;R companies to keep copies of data in overseas locations.</td>
</tr>
</tbody>
</table>

14. Navigating your digital transformation journey
1. Apply a data classification framework.
To navigate the restrictions applicable to seismic and drilling data, E&R companies can adopt smart policies that focus on the classification of data, establishing which data would fall within and outside the seismic and drilling data category. Having categorized data in this way, E&R companies can then put in place appropriate technical and operational measures to address concerns regarding seismic and drilling data (as will be outlined in points 2 to 6 below) and, in parallel, adopt cloud services for all other categories of data.

2. Understand where the data will be located.
The flow of data across borders is essential in this digital age. It is important that E&R companies consciously pick CSPs who can provide visibility on where their data will be hosted so that the necessary due diligence can be undertaken. The E&R company should also assess the applicable government policies, political, social and economic conditions, legal and regulatory developments, and the E&R company’s ability to effectively monitor the CSP. This is not only good practice; it ensures compliance with applicable data laws and regulations, which typically require that any overseas location provides, as a minimum, an equivalent level of protection to that which is available in the E&R company’s jurisdiction.

3. Ensure that the CSP has a policy on third party data requests.
A key concern for E&R companies when data is hosted outside of the E&R company’s jurisdiction, is the management of data requests from government bodies, law enforcement agencies or other authorities in the host country. To address this concern, the E&R company should only partner with a CSP that has a clear policy on third party data requests. This should include a commitment from the CSP to re-route any third party data requests to the E&R company itself, unless the CSP is legally prohibited from doing so.

4. Understand the CSP’s data security measures.
The CSP’s security policies, procedures and controls must protect the confidentiality and security of the E&R company’s data. This is essential, not just as a matter of good business practice and risk management but also to address regulator concerns regarding disclosure of, or unlawful access to, the E&R company’s data. For example, regulators in even the most highly-regulated industries such as financial services are increasingly acknowledging that securely encrypting data reduces risks associated with its storage and processing. By understanding the CSP’s security policies, procedures and controls, the E&R company will be in a good position to engage with the applicable regulator concerning the use of cloud services. We expand further on the issue of data security in the next section of this paper.

5. Understand the cloud deployment models available.
There are a variety of deployment models for cloud services. As part of the due diligence process, the legal and compliance team in E&R companies should ensure that they understand each deployment model and the specific configuration being proposed by the CSP.

Please see below a useful summary of the different types of cloud service and cloud deployment models:

Service models:
• Software as a Service (SaaS) where the CSP makes available software applications to customers;
• Platform as a Service (PaaS) where the CSP provides a computing platform for customers to develop and run their own applications; and
• Infrastructure as a Service (IaaS) where the CSP delivers IT infrastructure e.g. storage space or computing power.
Practical steps for E&R companies

Deployment Models:

- Public Cloud, where infrastructure is owned and managed by the CSP and located off-premise from the customer. Although the data and services are protected from unauthorized access, the infrastructure is made available to a variety of customers. Given the operational and commercial benefits to customers, public cloud is increasingly seen as the de facto deployment model.

- Private Cloud, where infrastructure is usually managed by the CSP (but sometimes by the customer). The infrastructure is located either on customer premises or, more typically, on the CSP’s premises. The infrastructure is exclusively available to a particular customer.

- Community Cloud serves members of a community of customers with similar computing needs or requirements. The infrastructure may be owned and managed by members of the community or by a CSP. The infrastructure is located either on customer premises or the CSP’s premises. The data and services are accessible only by the community of customers.

- Hybrid Cloud is a combination of two or more of Private Cloud, Public Cloud or Community Cloud.

6. Engage with the applicable regulator on seismic and drilling data if required.

Having implemented the measures described above, E&R companies will be in a good position to engage their regulator on the proposed use of cloud services in relation to seismic and drilling data. The discussion should focus on:

- the operational benefits of cloud services for the E&R company, as showcased in the various case studies in Part 1 of this paper and, in particular, the role that cloud services play in ensuring the competitiveness of the country’s E&R sector;

- the measures that the CSP has in place to address concerns regarding data location, security and third party access; and

- the different cloud deployment models available. For example, the E&R company may wish to explore with the applicable regulator whether, in relation to seismic and drilling data, hosting a local backup within the E&R company’s jurisdiction is an acceptable workaround.

Engagement should be a collaborative process involving both the E&R company and the CSP. The CSP should be on-hand throughout this process to provide detailed information about its cloud services in order to address questions or concerns from the regulator.

How Microsoft helps

Microsoft’s expert team is on-hand to support you throughout your cloud project, right from the earliest stages of initial stakeholder engagement through to assisting with any required regulator-engagement process. Our cloud product range spans all of the cloud service and deployment models described above which means our E&R customers have flexibility and choice. Through our expert knowledge in regulations and our extensive engagements with regulators, we are able to anticipate and address concerns from regulators even in the most highly regulated industries. We have also developed a range of resource materials including product fact sheets and online trust centres, designed to ensure that you have access to all the information needed to make an informed decision. In addition, we have subject-matter experts available to meet with you, your core stakeholders and, if required, your regulator, to provide specific and detailed information on the technical, contractual and practical aspects of any proposed cloud project.

Issue 2: Data Security and Privacy

Despite progress in cloud security standards and a growing acknowledgement that these can meet or even exceed security practices of on-premises solutions, concerns regarding data security persist. It is more important than ever that E&R companies partner with CSPs who have appropriate safeguards in place to protect even the most sensitive categories of data.

<table>
<thead>
<tr>
<th>Issue</th>
<th>A large portion of data held by E&amp;R companies is commercially sensitive and includes employee and contractor information which is subject to stricter privacy and data protection laws. Historically it is perceived, particularly amongst state-owned enterprises, that the use of third party technology services may result in a higher risk of security incidents or breaches which could result in contravention of privacy and data protection laws. Cautious of such perceived risks, some E&amp;R companies continue to maintain legacy on-premises infrastructure without realizing that their existing infrastructure may not comply with current security requirements.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reality</td>
<td>Existing on-premises solutions may no longer afford E&amp;R companies requisite level of security and privacy. Technological and operational advances mean that public CSPs such as Microsoft now have policies and controls that are on-par with or more advanced than many on-premises data centres of even the most sophisticated organizations. Companies, institutions and governments around the world use cloud services for even the most sensitive categories of data. This means that, with appropriate measures in place, E&amp;R companies can move to the cloud in a way that addresses all applicable security concerns.</td>
</tr>
</tbody>
</table>
| Practical steps for E&R companies | 1. **Perform a full risk assessment that considers any risks associated with the status quo.**  
Any new technology adoption should include a risk and benefit analysis. The failure by institutions to embrace new technologies may in itself increase risk and jeopardise competitive advantage. With this in mind, we believe that when the board and senior management are considering any risks associated with adopting new technology, the legal and compliance team should also advise on the risk of maintaining the status quo.  
2. **Assess the CSP’s security measures.**  
The CSP should be able to demonstrate that its security policies, procedures and controls adequately protect the confidentiality and security of customer information. One way to assess the CSP’s security measures is to consider whether they comply with international and the relevant country-specific standards. For example, ISO 27001 and ISO 27018 have become an expected minimum standard within highly regulated industries around the world. Aside from these international standards, the relevant country-specific standards include: CCSL (Australia), DJCP and TRUCS (China), CS Gold Mark and FISC (Japan), MeitY Accreditation (India) and MTC3 (Singapore). The evaluation of the CSP’s security measures should be backed up by independent third party audits to provide the E&R company with confidence that the CSP adheres to the strict security controls required by these standards. CSPs should also use encryption technology that meets or exceeds international standards to protect and secure the E&R company’s data at all times. In addition, in the context of a multi-tenant cloud solution, the data of one cloud customer should be separated from that of other cloud customers through measures such as logical separation. |

Practical steps for E&R companies

3. Consider privacy and data protection.

Although E&R companies process less personal data than other sectors such as retail or financial services, it is still essential that E&R companies comply with their privacy and data protection law obligations. In order to do so, E&R companies should understand from the CSP what privacy protections are built into the CSP’s services. For example, the E&R company needs to know (a) that the CSP will not use data stored on its cloud for purposes other than to provide the cloud service (such as advertising), (b) how long the CSP will retain the data and (c) how quickly it will notify the E&R company of any security incidents that affect the data. The E&R company should also review the CSP’s terms of service to ensure that they enable the E&R company to comply with its privacy and data protection obligations.

How Microsoft helps

Microsoft’s cloud services have been engineered with a focus on data confidentiality, security and compliance in mind:

1. Microsoft complies with national and international standards.

Microsoft cloud services meet a broad range of national, international, regional and industry-specific compliance standards, such as ISO 27001, ISO 27018, SOC 1, SOC 2, CCSL (Australia), DJCP and TRUCS (China), CS Gold Mark and FISC (Japan), MeitY Accreditation (India) and MTCS (Singapore). Independent third party auditors annually review Microsoft’s adherence to the strict controls set out within these standards.

2. Microsoft has tailored its security solutions for the industry.

For oil and gas companies, the Microsoft Upstream Reference Architecture (MURA)® provides a set of principles for establishing sound cybersecurity policies and procedures, tested and proven in real-world implementations, and designed to meet the specific requirements of the upstream oil and gas environment.

3. Security is built into the Microsoft cloud from the outset and each phase of development.

This starts with the Security Development Lifecycle, a mandatory development process that incorporates privacy and security requirements into every phase of the development process. Microsoft also uses various technological safeguards such as encrypted communication of data at-rest and in-transit to safeguard customer information.

4. Cybersecurity driven by data analytics.

Microsoft uses its rich analytics engines driven by threat intelligence to offer an even more sophisticated level of protection to customers. By applying a combination of automated and manual processes, machine learning and human experts, Microsoft has created an intelligent security graph that learns from itself and evolves in real-time, reducing the time taken to detect and respond to new incidents across products.

5. The Microsoft cloud is build with privacy and data protection in mind.

For example, data that resides in Microsoft’s cloud services belongs to the customer, not Microsoft. Microsoft’s contractual terms are clear that the customer retains ownership of all data stored in the Microsoft cloud. Microsoft also uses the customer’s data only to provide services that have been agreed upon. If the customer leaves the Microsoft cloud, strict standards and specific processes are triggered to remove the customer’s data from Microsoft’s systems. Microsoft also takes robust measures to protect the customer’s data from inappropriate access, including imposing access limitations on Microsoft personnel and subcontractors. The customer, however, is free to access its data at any time and for any reason. You can access more detailed information about the robust security and privacy features at the core of each Microsoft cloud service in the Trust Centre.6

## Issue 3: Business Continuity

It is essential that the E&R company's operations are not disrupted in the event of a CSP service failure. Service disruption not only interrupts the E&R company’s business but can also give rise to health and safety or environmental concerns. Cloud services therefore need to be reliable and the CSP should have appropriate business continuity measures in place to prevent disruption and to promptly deal with it if it occurs.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Practical steps for E&amp;R companies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The E&amp;R company must be able to continue conducting its operations even in the event of a service disruption. Any outsourcing arrangement should therefore take into account the business continuity risks associated with the proposed service provider.</td>
</tr>
<tr>
<td>Reality</td>
<td>Business continuity management sits alongside security as a cornerstone of trust in any technology project. Business continuity concerns should not, however, be a barrier to the use of cloud services. As with data security, there is growing acceptance that cloud services from providers such as Microsoft include business continuity procedures that are on-par with or more advanced than those of even the most sophisticated organizations.</td>
</tr>
<tr>
<td>1. Obtain binding contractual commitments as to service availability.</td>
<td>The CSP should provide the E&amp;R company with a Service Level Agreement, setting out service availability expectations. Service Level Agreements should include financial guarantees in the event of a failure to meet the required standards.</td>
</tr>
<tr>
<td>2. Ensure that the CSP has robust incident management processes.</td>
<td>The E&amp;R company should check that the CSP has robust incident management processes to ensure that the E&amp;R company is prepared for all possible scenarios. This should include a process for the CSP to promptly respond to any security issues if they occur and to notify the E&amp;R company if they become aware of any unlawful access, loss, disclosure or alteration of customer data.</td>
</tr>
</tbody>
</table>
3. Address business continuity plan testing.
The E&R company should check that the CSP carries out regular and meaningful business continuity plan testing. Issues identified during tests should be noted and managed to a resolution.

4. Ensure that the CSP offers service monitoring tools.
The E&R company should ensure that the cloud service includes tools that enable ongoing examination, verification, access and control of the cloud services, so that the E&R company can track performance. The CSP should provide real-time and continuous information about the current availability of services, history of availability status, details about service disruptions and outages, and scheduled maintenance times.

How Microsoft helps
Microsoft provides a range of tools to ensure that E&R companies’ operations will not be disrupted in the event of a service issue. The Microsoft Enterprise Business Continuity Management (EBCM) program is based on the Disaster Recovery Institute International Professional Practice Statement and the Business Continuity Institute (BCI) Good Practice Guidelines. Our EBCM program applies across Microsoft’s business and drives the development of business continuity plans for our individual cloud services in line with industry best practices. In addition to our own rigorous program, we also provide mechanisms for customers to control backup and recovery themselves. For example, Azure Backup provides the ability to back up and restore virtual machines.

We also have robust security incident-management processes. The Microsoft Security Incident Management (SIM) team, which is responsible for assessing and mitigating computer security incidents, will promptly respond to any potential security issues as and when they occur. We make binding commitments to notify customers if we become aware of any unlawful access, loss, disclosure, or alteration of customer data.

Finally, we provide tools to enable ongoing monitoring of performance. Service health can be monitored through publicly available sources. This information helps you assess our performance against our binding contractual Service Level Agreements, which provide financially backed availability guarantees.
Part 3: Legal and compliance professionals as drivers for digital transformation
The changing roles of legal and compliance professionals

As the E&R sector shifts towards new technologies, the role of legal and compliance professionals is more critical than ever before. The legal and compliance community is involved in all aspects of digital transformation, from supporting technology procurement and due diligence processes to advising on regulatory changes and cybersecurity risk.

Moving into new and uncharted territory represents an enormous opportunity for legal and compliance professionals — namely, the opportunity to drive the digital transformation of their organization, and be at the forefront of these developments at a time when the industry is changing faster than ever before. Forward-looking legal and compliance teams must not be daunted by the prospect of needing to understand a rapidly-changing legal and regulatory environment that deals with new and emerging technologies. They should instead see the opportunity not just to react to the digital transformation but to shape it and, by doing so, provide their organizations with a powerful competitive advantage.

Through our long-standing relationship with the legal and compliance community, Microsoft understands the challenges that professionals face. In this section, we provide some insights on how high-performing legal and compliance teams across sectors and jurisdictions drive digital transformation and deliver a competitive advantage to their organizations.
Delivering a competitive advantage: opportunities for legal and compliance professionals

Understanding the changing definition of “risk”

The first and most important step for legal and compliance professionals working on digital transformation projects in the E&R sector is to recognize that the definition of “risk” has changed. In the past, risk often meant doing something new or different, such as adopting a new or emerging technology. Today, high-performing legal and compliance teams recognize the risk of standing still. Not only will E&R companies that stand still be overtaken by more agile competitors, they may actually be exposed to a higher level of regulatory risk (for example, E&R companies that fail to leverage the latest technologies may be more exposed to threats such as cyber-attacks). High-performing teams recognize this important paradigm shift and build the risk of standing still into all aspects of their thinking and advice.

Creating clarity for the organization

The rapidly changing technology and regulatory environment can seem overwhelming. Many digital transformation projects are held up, even where there are strong commercial drivers to proceed, because the way forward appears littered with potential hazards, whether real or perceived. The situation is often compounded by the introduction of new laws and regulations, such as the EU’s General Data Protection Regulation (GDPR) or China’s Cybersecurity Law (CCL). In this environment, high-performing teams step forward to create clarity for the E&R company. They recognize that, at the core of any digital transformation project are only two moving parts — the technology solution, and the legal and regulatory framework. They focus first on understanding the technology because they recognize that, once it is de-mystified, it is much easier to assess against the legal and regulatory environment. Many organizations are therefore investing in re-skilling their legal and compliance professionals to become digital experts, as well as legal experts.

Having understood and de-mystified the technology solution, it often becomes clear that the legal principles that apply are the same ones that legal and compliance professionals are already familiar with. For example, data protection and cybersecurity laws will exist, and new ones will continue to be introduced, regardless of whether a business makes use of new technologies. What changes is the way in which those rules apply in respect of matters such as cross-border transfers of data. By understanding the technology, mapping it against the legal and regulatory environment, and leveraging the experience of their technology partners (who will likely have substantial experience navigating new requirements such as GDPR and CCL with their customers), legal and compliance professionals are well-placed to chart a course and lead the organization through the digital transformation process.

Successfully partnering with other teams

Successful digital transformation projects cannot be delivered by the legal and compliance team alone. High-performing legal and compliance teams take steps to put in place a more collaborative working relationship with other parts of the organization:

• They engage with the leadership to understand the innovation agenda, reflect on strengths, weaknesses, vision and objectives, and discuss risk profile and tolerance. By understanding the commercial context, the legal and compliance team will not only be prepared to more accurately prioritize concerns, but also be empowered to craft practical, bespoke solutions that continue to achieve the organization’s strategic goals.

• They build and lead multi-disciplinary teams with other parts of the organization — including, in particular, the IT and procurement teams. Unfortunately, digital transformation projects can often be held up when the legal team is involved at the last minute to “paper” a solution that may not be the right fit from a legal and regulatory perspective. By building and leading a multi-disciplinary team, legal and compliance professionals ensure that they are involved and can shape the process from the outset.

Through these strategies, legal and compliance professionals can build a reputation within the organization as an enabler and a collaborative force, not an obstacle to innovation.
In conversation with Alex Westmoreland

Alex Westmoreland is Legal Counsel in the Marketing, Technology & Supply legal team at BHP based in Singapore. Alex supports the Technology and Supply functions at BHP, advising on a wide range of matters including adoption and implementation of new technologies in line with BHP’s technology strategy, software licenses, commercial contracts, IP, data privacy and open source software.

How has your role as legal counsel changed given the increased focus on digital transformation in the E&R industry?

As the pace of digital transformation has picked up at BHP, moving towards our goal of a fully integrated and highly automated organization, I have had the opportunity to become much more embedded in the project teams driving the work. I have developed strong relationships with the technology function and am relied upon as a trusted advisor at each step of the process. I have also needed to become more focused. Given the scope and scale of change involved in digital transformation, there can naturally be a lot of noise around the fringes as everybody sets about delivering it, which I have learned to tune out to focus on the areas that, as a legal advisor and strategic partner, I can bring the most value to.

How do you drive the rollout of digital transformation solutions in your organization?

I have learned to be cognizant of, and adapt my advice to take account of, the legal risks associated with digital transformation and be pragmatic in working with the business to find ways to deliver projects in line with that advice, without becoming a roadblock to progress. The important part is to fully understand the goals of the business, and the opportunities that are being pursued, thinking of the bigger picture as well as the speedbumps that crop up along the way, which significantly helps in overcoming them. Digital transformation is a collaborative effort, so synergy between the legal, technology and other functions is essential for a successful outcome.

How should legal and compliance professionals upskill themselves in order to better support their organization in digital transformation deals?

There are many ways this can be achieved, but certainly take advantage of the opportunity to speak with others inside and outside the industry who are going through the same process to share ideas (where not prohibited by law/regulation of course!). Spend time around the technology teams, perhaps shadow them or do a short-term secondment so you can understand the objectives and processes from their perspective. This greatly enhances the possible level of collaboration between the functions, which in turn increases the chances of success.
Conclusions

At this time of digital transformation in the E&R sector, it is crucial that forward-thinking industry players explore the opportunities presented to them by today’s technological advances. The legal and compliance teams must recognize their changing roles as agents of change and should proactively support their company’s digital transformation endeavours. An overly cautious and risk averse legal and compliance team that is unduly concerned with perceived regulatory barriers may stymie an otherwise beneficial digital transformation deal.

As expounded upon, these barriers are all but illusory and there are practical solutions to working around regulatory boundaries. This is not to say that legal and compliance teams should recklessly rubber stamp all digital transformation deals. Consideration must be given to the business goals of the company and whether digital transformation solutions offered would provide business advantages to the company. To do so, the legal and compliance team, together with the relevant business groups, must engage CSPs which have in-depth expertise to advise them on digital transformation.

By overcoming these perceived barriers and executing their digital transformation strategies, we believe that E&R companies in Asia-Pacific can become thriving digital businesses that sustainably provide energy, metals, minerals and raw materials to fuel economic prosperity in the region.

This paper is part of Microsoft’s commitment to helping customers in the Asia-Pacific E&R sector overcome perceived barriers and adopt new technologies in a way that meets all applicable risk and compliance requirements. We look forward to hearing your digital transformation success stories.
Further Information

Find out more

Trust Center
microsoft.com/trustcenter

Navigating your way to the cloud
microsoft.com/en-sg/apac/trustedcloud

Service Trust Portal
aka.ms/trustportal

Online Services Terms
microsoft.com/contracts

SAFE Handbook
aka.ms/safehandbook

© Microsoft Corporation 2018. All rights reserved. Microsoft, the Microsoft logo, Azure, Dynamics, Intune and Office 365 are either trademarks or registered trademarks in the United States and/or other countries. This paper is not intended to be a comprehensive analysis of all regulations and their requirements, nor is it legal advice; rather, it is intended to be a summary and to provide guidance to energy and natural resources companies on the types of issues they should consider. 19634/1118