KILPATRICK TOWNSEND

6 KEY TAKEAWAYS

SaaS, PaaS, and IaaS: Evaluating Cloud Service Agreement Models, Negotiating Key Terms, & Minimizing Contract Disputes

Kilpatrick Townsend Associate Megan Demicco recently participated in a webinar that provided guidance to business and technology counsel concerning drafting cloud computing service agreements.

6 Key Takeaways from the presentation include:

1. For businesses evaluating whether to move services to "the cloud," it's important to consider the transaction risk profile. Is this a "nice to have" business tool, or a mission critical application? As the criticality of the services at issue, or the sensitivity of the data to be hosted in the cloud increases, the risk of moving a particular service to the cloud increases.

2. Cloud service agreements should clearly reflect the scope of services being contracted for. Identify upfront whether any customizations may be needed; cloud providers generally limit customizations so they can more efficiently manage services and provide a scalable solution.

3. Ensure service level agreements measure the relevant metrics, and that associated credits appropriately incentivize the provider to perform. If a provider won't negotiate the SLA metrics or credits, consider asking for a right to terminate for repeated or chronic service failures.

4. While data privacy and security in the cloud is never absolute, you can take steps to protect your business. Agreements should: (i) clearly outline permitted and prohibited provider uses of your data, and storage and access requirements; (ii) require provider compliance with applicable data security laws, industry best practices, and in some cases independent security standards or your internal policies; (iii) specify your audit rights; and (iv) outline the provider's response requirements in the event of a breach.

5. Using the business model (one to many) as justification, cloud agreements typically offer very limited liability for the provider. Negotiate liability where you can given your relative bargaining power. You can also mitigate risk by choosing a cloud provider with a good track record and a strong reputation. Cyber liability insurance can be helpful but note coverages and policies vary widely.

6. Contemplate the end at the beginning. Be aware of provider rights to suspend or interrupt services, and to terminate early, and limit these if possible. Consider if you need assistance migrating data to a new provider and contract for this up front. Require the provider to give you access to your data, in a usable format, for a reasonable amount of time after termination.

Megan Demicco focuses her practice on outsourcing agreements and technology licensing. Prior to joining Kilpatrick Townsend, Ms. Demicco was Assistant General Counsel at the Texas Department of Information Resources where she served as the primary state attorney for Texas.gov, the state's eGovernment portal, a public-private partnership offering more than 1,000 online services for more than 100 publicly-funded customers.

For more information, please contact: Megan Demicco at mdemicco@kilpatricktownsend.com.