ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Risks and Remedies: Cloud Computing and Software Licensing

Commercial and Contracts

Technology, Privacy, and eCommerce

A shift to cloud computing has altered how the world does business, providing cost-effective alternatives to traditional on-premise solutions while continuing to offer flexibility and security. Nonetheless, as corporate technological infrastructures increasingly depend on “software-as-a-service” solutions, a successful information technology strategy requires a careful examination of the challenges and risks associated with these offerings.

In a series of articles, we will examine how cloud-based software solutions compare to traditional on-premise software solutions, explore the common cloud service delivery models, and discuss the legal toolbox — including warranties and service levels, data security and confidentiality obligations, as well as indemnities and limitations of liability — needed to protect businesses and their bottom line. But first, we delve into effectively weighing the pros and cons of various computing and licensing options.

Different organizational requirements, resources, and capabilities need distinct technical features and support, which requires careful selection of service providers and solutions. Perhaps a turnkey solution that implements and manages updates and user validation will provide the best results. Alternatively, a customized solution that provides refined ability to control discrete items such as access management, maintenance, and support may be required. As both on-premise and cloud-based solutions offer these and many other configurations, identifying primary strategic goals is key to informed selection and successful implementation.

Baseline questions address some obvious distinctions between on-premise software and cloud-

based solutions. Ask the following:

- Does the company need to eliminate costs related to procuring and maintaining hardware and infrastructure?
- Have vulnerabilities been identified that necessitate a security lock down and improved access control?
- Does the company have the resources and experience to manage these activities in-house? Even if it does, are there reasons it would prefer not to do so?

While the answers to these questions may initially favor one licensing structure over the other, a thoughtful analysis will also address the following five considerations: purpose, users, rights, risk, and remedies.

Purpose

Determine the purpose and relative criticality of the business activities that the solution must support. In a traditional on-premise software environment, a company may exercise greater control over infrastructure, implementation, and support, including ensuring appropriate redundancies; however, in cloud-based solutions, this control is typically held by the service provider. While some companies may prefer to manage an on-premise solution for mission-critical or highly visible functionalities, not all have the internal expertise or resources to do so. Regardless of the environment, responsibilities allocated between the service provider and the company must collectively support the intended purpose and required level of business continuity, including availability and uptime, service quality, data integrity and security, and rights upon contract expiration or termination.

> While some companies may prefer to manage an on-premise solution for mission-critical or highly visible functionalities, not all have the internal expertise or resources to do so.

To determine the purpose and relative criticality, consider:

- Will the solution support internal or back-office operations, or transactions between the company and its customers?
- Will its implementation be invisible to the outside world, or obvious and associated with the company’s public presence and brand?
- Is the solution a sole-sourced or critical functionality that is essential to business operations, or an optional, nice-to-have but not essential functionality? In either case, can it be easily discontinued or replaced without significant business disruption?

Regardless of the environment, responsibilities allocated between the service provider and the company must collectively support the intended purpose and required level of business continuity, including availability and uptime, service quality, data integrity and security, and rights upon contract expiration or termination.

Users

Identify each population of users who needs access to or benefits from the solution. Under almost any licensing model, a company must monitor its entitlements, deployments, and usage to ensure that it remains compliant with the scope of the license granted. If the scope of a traditional software

license is exceeded, even if by mistake, a formal and even an informal audit may result in hefty fees and costs, suspension of support, and threats of termination. In a cloud-based solution, entitlement management is effectively outsourced to the service provider, who can also unilaterally revoke access to the services. Moreover, while it is equally important for compliance purposes to authorize the correct user population for on-premise and cloud-based solutions, keep in mind that unauthorized use may be more easily detectable in a cloud environment. Therefore, it is important to ensure the solution meets the organization's anticipated needs.

Privacy and data security

Privacy and data security should be prioritized in both on-premise software and cloud-based solution licensing. Cloud computing introduces additional implications for data, such as where the data is stored and whether the data is encrypted while in transit or at rest. In the world of cloud computing, data may flow across borders as a normal part of the service provider's processing. Due diligence should be conducted to determine whether a cloud service provider is appropriately certified and capable of maintaining the integrity of data. If the service provider is using a third-party platform or will subcontract any services, consider where the data will be stored, who will have access to the data and from what location, and whether data permissions allow the licensee company to provide this access.

Rights

Secure the full set of rights needed to support your business case. An effective checklist matches a company's intended usage, users, and manner of implementation against both statutory copyright rights and additional contractual rights needed to meet the company's business requirements. While each item on the checklist may not apply to all on-premise software and cloud-based solutions offerings, testing each issue will optimize your ability to exploit the license in the context of your business environment.

License grant

At a minimum, the license grant must secure each of the rights needed to copy, modify, or prepare derivative works, distribute, and publicly perform and/or display the solution in pursuit of the company's purpose. A comprehensive license grant will specify (1) permissions or restrictions concerning geographies, sites, devices, and users; (2) conditions to sublicense or transfer; (3) all

rights needed to support the company's contractual obligations to its customers or other third parties, such as the right to audit a cloud service provider's data security measures; (4) events that trigger the right to terminate the license; and (5) whether any rights, and obligations, survive expiration or termination.

Termination rights

In many respects, an analysis of termination rights for cloud-based solutions offered on a subscription model typically resembles that for an on-premise software license. However, there are some key distinctions in the areas of service suspension and termination.

While a company with an on-premise software solution generally retains access to and control of its data at all times, a company that elects to upload, maintain, or transact its data in the public cloud largely cedes this control to the service provider. It is important to examine the cloud service provider's right to suspend access or services and negotiate appropriate notice and limitations based on business needs. If a service provider terminates the services, termination may create a significant disruption to its business, especially if a company is not prepared with an alternative.

Conversely, a company should consider whether business sensitivities require a right to immediately discontinue the service and the service provider's access to its data upon certain events, such as a competitive acquisition. Finally, cloud subscription agreements often provide only a short window during which the company can recover its data that has been maintained in the cloud under the service provider's control.

A company seeking a longer period or rights to access and validate its data during the term will have to negotiate these rights. As with on-premise software, the company must ensure compatibility to make meaningful data export rights on termination and transition. Addressing these issues at the beginning of the relationship reduces uncertainty and provides a path to mitigating risks associated with the solution.

Risk

While one can never contract risks away entirely, choosing a licensing model that meets a company's business requirements, suits its environment, and appropriately allocates responsibilities between the parties is the best way to minimize exposure. While cloud solutions can provide comprehensive and efficient services that meet multiple business objectives, it is important to consider how the shift in control over systems and data may pose both similar and different risks for operations and potential exposure to third parties.

> While one can never contract risks away entirely, choosing a licensing model that meets a company's business requirements, suits its environment, and appropriately allocates responsibilities between the parties is the best way to minimize exposure.

Under a cloud solution license, a company will lose a degree of control and visibility into the solution and must rely on its service provider to maintain those policies, infrastructure, and security as described (and only as described) in the contract.

Moreover, a company does not completely absolve itself of all responsibility: For example, it will still

be responsible and liable to the licensor in the event its credentials become compromised, and to its own users and customers for failures respecting data integrity, security, and retention. Negotiating business-focused, customer-friendly rights mitigates the risks associated with each solution and integrates sufficient remedies to address any issues that arise.

Remedies

Identify meaningful remedies that will promote business continuity. In the cloud environment, examine service availability or uptime commitments carefully, be wary of loosely defined “unscheduled maintenance” exceptions, and consider whether the service provider’s technical support hours and schedule align with the company’s business needs.

The right to terminate the license for a cloud solution due to service level failures may be effectively meaningless without rigorous transition support, and may be bolstered by escalating obligations directed at minimizing business disruption.

As discussed above, data security remains a highly important issue in the cloud environment and, unlike an on-premise solution, may involve not only the licensee company and service provider, but also a third-party platform provider on which the cloud solution is hosted. A clear, actionable plan that allocates responsibility and liability should be in place to respond to any data security breach and mitigate the damage. And as with any solution, organizations should maintain the right and flexibility to in-source, outsource, and back up services so that its business does not become too dependent on any single solution.

As the technology fueling businesses rapidly advances, the issues related to its implementation and use continue to evolve as well. Considering the fundamental issues of purpose, users, rights, risks, and remedies provides an organization with key information to navigate the increasing complexity and sophistication of on-premise and cloud solutions offerings to make informed and effective decisions.

Sarah Beisheim

Legal Counsel

REMADE Institute

Sarah Beisheim is legal counsel for REMADE Institute, a Manufacturing USA® Institute and division of Sustainable Manufacturing Innovation Alliance Corp. She previously spent more than 24 years with Xerox Corporation, where she was senior IP counsel and lead product counsel focusing on complex commercial and intellectual property transactions.

William Eipert

Senior Counsel and Lead Advanced Development Counsel

Xerox Corporation

William Eipert is senior counsel and lead advanced development counsel for Xerox Corporation counseling Xerox's research and product development organizations across a range of strategic intellectual property and commercial transactions including acquisitions, divestitures, outsourcing, licensing, joint development, sponsored research, and OEM arrangements.

Farah Cook

Partner

Kilpatrick Townsend & Stockton, LLP

Farah Cook is partner at Kilpatrick Townsend & Stockton, LLP. She concentrates her practice on technology-focused commercial agreements, marketing technology arrangements, advertising technology, and licensing of intellectual property, strategic alliances, content distribution, and innovative cloud and data products.
Her combination of in-house and big law firm experience, as well as her broad practice, gives her the ability to creatively and efficiently identify, understand and navigate issues in technology, commercial and marketing matters.

Jeff Connell

Associate

Kilpatrick Townsend & Stockton, LLP

Jeff Connell is an associate at Kilpatrick Townsend & Stockton, LLP. He focuses his practice on information technology, business outsourcing agreements, systems integration, software as a service (SaaS) transactions, technology licensing, cybersecurity, data privacy and other technology and commercial transactions. Prior to joining Kilpatrick Townsend, Jeff was an associate in the Atlanta, Georgia office of an international law firm where he advised clients on technology transactions and corporate law.

Stacie Greskowiak McNulty

Director and Counsel

HOPE Cape Town USA

Stacie Greskowiak McNulty is director and counsel of HOPE Cape Town USA. She most recently served as general counsel for Orbital Effects/R2 Space, a private company providing cutting-edge radar satellite technology and related applications to the United States government. She also previously served as senior legal counsel and director of litigation at Marconi Group/PanOptis, where she developed and executed highly successful global litigation strategies in patent infringement cases, contract and commercial disputes, and competition matters.