Skadden

Outsourcing: Maximizing Value and Mitigating Risk in 2015

Contacts

Stuart D. Levi
212.735.2750
stuart.levi@skadden.com

Jessica N. Cohen
212.735.2793
jessica.cohen@skadden.com

James S. Talbot
212.735.4133
james.talbot@skadden.com

Four Times Square
New York, NY 10036
212.735.3000

On April 21, Skadden presented a seminar titled "Outsourcing: Maximizing Value and Mitigating Risk in 2015." Areas of focus for this year included: service-level structure and optimization, liability coverage, and privacy and cybersecurity. The Skadden panelists were Jamie Talbot, Jessica Cohen and Stuart Levi, who are members of the firm's Intellectual Property and Technology, Privacy and Cybersecurity, and Outsourcing practices. Stuart is co-head of Intellectual Property.

Service-Level Structure and Optimization

Jamie focused on how vendors and customers can use service levels as a management and governance tool for outsourcing agreements. In an environment where both customers and vendors know a service is unlikely to be perfect all of the time, service levels establish the expected standard of performance and measure whether these standards are met.

Service-level standards can be set using various metrics, including system uptime, error resolution time and customer satisfaction — though Jamie cautioned against relying on customer satisfaction surveys because the results may be too nebulous and therefore unfair to the vendor. Service levels also can be put into different categories, such as "Critical Service Levels" and "Key Performance Indicators," that may have different meanings. Key Performance Indicators, for example, may be for reporting purposes only with no service credits attached for failure to meet the designated standard.

Jamie highlighted that vendors recently have been asking customers to select fewer service levels as opposed to designating everything that is measurable as a service level. This allows vendors to limit the burden that measuring and tracking service levels places on their operations, while customers benefit because the vendor's attention is focused on the aspects of the service that matter most to them.

Jamie also emphasized that customers should be realistic about the service levels they expect vendors to achieve; otherwise, vendors may build the cost of failing to meet an impractical service level into its base pricing model. Initial service levels can be agreed to based on a variety of approaches, ranging from carrying forward the customer's prior service levels when it performed the service to using industry or vendor standard levels to measuring service performance over the initial service period and using the results. This last approach has risks, however, as it encourages vendors to reduce service performance in order to lock in low service levels. It also takes place over the time when initial problems with the services are identified and worked out, which may skew the results lower.

Service-level credits are payments made by the vendor to the customer when the vendor fails to meet certain service levels. They usually are based off a percentage of fees paid throughout the term of the outsourcing agreement. Agreements also often include a cap on service credits known as the "at-risk amount." Jamie noted that, while the at-risk amount can range between 5 percent and 20 percent of the total fees, the 10 percent to 15 percent range is typical. Vendors may allow customers to allocate a percentage of the at-risk amount between the different service levels using the concept of an "allocation pool." With this method, customers can designate a percentage of the at-risk amount for each service level. The total allocation pool will mathematically exceed the total at-risk amount, but the at-risk cap still applies. Although this means that if services fail a range of different service levels in a particular period the customer will not receive the full service credits, it allows the customer to assign greater weight to individual service levels. Ultimately, this allows customers to designate what is most important to them while still giving vendors certainty in their risk model.

Some outsourcing agreements allow vendors to earn back service-level credits that the vendor paid if, for example, the vendor then exceeds the service level or does not breach the service level for a set period of time. Customers may see this as an incentive for getting the vendor to resolve issues. In practice, however, Jamie noted that earnbacks often do not make sense for the customer. The vendor essentially is getting a "free pass" for one service-level failure if the vendor assumes it can earn the credit back. Furthermore, the customer often does not benefit from performance above the service level and therefore has no reason to offer a financial reward for it. Finally, if the customer is actually harmed, the earnback deprives the customer of a portion of the compensation owed.

In general, service-level credits are the sole remedy for breach of a service level, as long as the performance is within the designated band where specific remedies have been established. Vendors and customers also can establish additional bands and remedies for failures that are short of termination. Ultimately, the parties should work together to determine when the termination should apply.

Jamie also pointed out that increasing service levels based on average performance over time is not an effective way to manage the vendor. The increase punishes the vendor for good performance and encourages vendors to perform exactly at the designated service level during the measuring period, even if higher levels could be achieved.

Outsourcing agreements also include a "burn-in" period during which service levels are measured but no service credits apply. This period typically begins when the services have been transitioned to the vendor (after any initial implementation or transition period) and continues for a few months. This approach allows the vendor some time to work out any problems in the service but avoids the uncertainty of setting service levels and credits later in the agreement.

Liability Coverage

Jessica began by noting that the standard liability structure of outsourcing agreements has begun to shift as such agreements have become more complex and vendors are more cognizant of their risks and liabilities. Outsourced services are subject to increased regulatory scrutiny. Regulators review outsourcing agreements and require the parties to specifically allocate liability for certain issues. The standard indemnity structure (mutual, uncapped and applicable to third-party claims only, with the indemnifying party controlling the defense) has now shifted. Indemnification now often covers direct damages for certain types of claims, subject to a cap. For some claims, particularly those by regulators, the indemnified party is allowed to control the defense of the claim. Jessica noted that the shift in who controls the defense of the claim is due to indemnified parties that are regulated entities wanting to maintain control over relationships established with the regulators. Regulated entities often have longstanding relationships with the regulators, and many do not want to risk that relationship being adversely affected by the indemnifying party.

Jessica pointed out that the standard liability cap on direct damages of 12 months of fees also has begun to shift. Parties are specifying different caps for certain types of damages, including breach of confidentiality and security issues. She emphasized that both parties should thoroughly assess the real risk of harm and liability before setting the cap, rather than having the mindset that special caps will simply be double the standard 12 months of fees.

Finally, Jessica discussed an alternative liability structure. Some vendors and customers create a pool of money allocated for the customer to use to make their clients whole in the event that a vendor's mistake causes the customer's clients harm. These "fat finger provisions" are useful when a customer's agreements with its clients isolate the customer from liability but the customer still wants to compensate its clients to retain their business. The amount should be tied to the customer's historical compensation rates with regard to these types of mistakes and can sometimes include a deductible in an amount that the customer is willing to bear. This type of provision ensures that the customer is satisfied and able to work well with its clients while also helping the vendor limit its liability for these discretionary payments to a predetermined amount.

Outsourcing: Maximizing Value and Mitigating Risk in 2015
Key Takeaways

Privacy and Cybersecurity

Stuart emphasized that hackers often use vendors to penetrate customers' systems, and vice versa. In addition, regulators are increasingly focused on how companies manage their vendor cybersecurity risk. Stuart pointed to several recent regulatory actions that highlight regulators' focus in this area. For example, the Federal Trade Commission brought a Section 5 claim against GMR Transcription Services because the company failed to monitor its vendor's cybersecurity measures. The New York Department of Financial Services and the Financial Industry Regulatory Authority (FINRA) also have highlighted the cybersecurity risk posed by vendors in their cybersecurity guidance. As a result, cybersecurity provisions in an outsourcing agreement no longer should be relegated to boilerplate provisions. Rather, companies need to focus on these issues in light of the specific vendor and the risk profile it presents. Stuart emphasized that both customers and vendors will benefit from discussing cybersecurity risk allocation early on in the negotiation of an outsourcing agreement.

With respect to the level of cybersecurity protection to require from a vendor, Stuart strongly cautioned against relying on where the vendor is located or the size of the engagement. Rather, the risk assessment should be based on the extent of the access each party may have to the other's network. Stuart also noted that companies should look at what data and information a hacker *could* access through the vendor's connectivity, even if the vendor itself might not use such data or information.

When negotiating the cybersecurity provisions of an outsourcing agreement, the parties should strive to avoid ambiguous or undefined concepts or language. For example, Stuart explained that an obligation to "remain current with industry standards" can be interpreted numerous ways by parties acting in good faith. Instead, companies should drill down on that definition, understand each side's expectations and draft the provision accordingly. Similarly, parties should be specific on the types of audits they will require and the amount of cybersecurity training they expect the other party to engage in.

Perhaps most importantly, the parties should have certainty surrounding their respective obligations to notify the other about cybersecurity attacks. For example, parties should know whether they are obligated to report all attacks or just those affecting the other party. The parties also should specify whether a party in the midst of dealing with a cyberattack has an obligation to keep the other party updated on material developments in mitigation and remediation. Finally, the parties should set forth the procedure for notifying consumers of attacks, including who makes the final decision.

Stuart pointed toward allocation of liability as the most hotly negotiated issue regarding cybersecurity in outsourcing agreements. There is a real risk of harm in today's environment, and damage could be significant. Unfortunately, much of this damage is intangible, such as damage to reputation. Stuart re-emphasized Jessica's point that the liability structure warrants a meaningful discussion, and parties should not simply rely on a multiplier of service fees. Stuart suggested that the parties specify the damages that are to be covered and then link the liability cap for cybersecurity attacks to the risk presented. Companies also should consider whether they have cybersecurity insurance that might mitigate the risk.