INDUSTRY DEVELOPMENTS AND MODELS

Vendor and Sourcing Management: Maintaining Control of Vendor Relationships by Avoiding Vendor Lock-In

Aaron Polikaitis

IDC OPINION

Globally, with perhaps a few minor exceptions, enterprises are free to choose the vendors that provide information technology (IT) products and services used to operate and grow their businesses. Accordingly, it would be expected that the chosen IT vendors would do everything within their power to ensure that every business need of their customers is met, regardless if required by contract. After all, if a customer is free to choose another vendor, why wouldn't the incumbent vendor do everything it can do to keep the business? Nevertheless, all too often, vendors act in their best interest and not in the interest of their principals, the enterprise customers. A few examples of this behavior include discontinuing software products without clear road maps for replacements, releasing products without the appropriate quality checks, charging excessive fees to fix their own bugs, changing license models causing sharp increases in fees, developing economically unsupportable solutions, and outsourcing support services to untrained individuals. Why then, if in the age of deregulation and freedom of choice, do large corporate entities continue to finance vendors (their agents) that put their own interests in front of their principals? In this study, IDC:

- Identifies factors which influence vendor behavior
- Evaluates how vendor lock-in eliminates a customer's freedom of choice and leverage with its incumbent vendors
- Provides advice on how to identify and reduce vendor lock-in situations

IN THIS STUDY

This IDC study provides guidance to CPOs and CIOs struggling to manage the most common pitfalls encountered in their relationships with external suppliers. It provides key strategies for minimizing negative behaviors common to outsourcing suppliers. Furthermore, this study guides vendor sourcing and management organizations (VSMOs) in making strategic plans for new relationships with vendors providing 3rd Platform technology solutions. These plans will help the enterprise avoid making technology and vendor decisions in pursuit of short-term gains without appropriately assessing the negative long-term implications of such decisions. Although 3rd Platform technologies and delivery methods have changed, this study applies lessons learned from vendor relationships formed for 2nd Platform technology solutions to key 3rd Platform technology procurement considerations.

IT Executive Program Research Agenda

This IDC continuous research program is focused on the issues, challenges, and opportunities confronting business and IT practitioners. Our research agenda is founded on the strategic goals that inform our research objectives. At the heart of our planning process is the need to balance the state of

August 2015, IDC #258202

established best practices with the pressing needs of our clients as they confront emerging technology management challenges. Our agenda is organized around 12 major themes (see Figure 1).

FIGURE 1

IT Executive Program Research Agenda Themes

The 12 Strategic Themes	
IT Strategy and Innovation	Infrastructure and Cloud
Strategic Architecture	Data Management
Application Development	Enterprise Mobility
Integrated Services Transformation	IT Security
Vendor and Sourcing Management	Customer Experience
IT Talent Management	Big Data/Analytics

Source: IDC, 2015

SITUATION OVERVIEW

Prior to 1984, consumer and commercial customers had to rely on a single vendor, affectionately referred to as Ma Bell, for telecommunications services. At the urging of many economists, including Milton Friedman, author of *Free to Choose,* the Bell system was broken up. Turn the clock forward 35 years and the landscape has changed dramatically. After decades of antitrust litigation, consumers and commercial customers are now free to choose who provides their telecommunications and every other information technology product and service. The number of vendors providing such products and services is staggering. As Table 1 shows, in 2014, $3.4 trillion was spent with thousands of vendors. With customers' freedom of choice and large number of vendors to choose from, why do some vendors (agents) in some situations act in their own best interest, rather than in the best interest of their customers (principals)?

TABLE 1

Vendor Count

2014 Worldwide Spending	$(B)	Vendors
Telecom services	1,558	500
IT services	646	1,000
Mobile phones	414	35
Software	407	2,000
Desktops, laptops, and tablets	274	50
Servers and storage	88	25
Printers	58	25
High-end server/mainframe	8	10

Source: IDC's *Worldwide Black Book* (1Q15), Trackers (1Q15), and *Global Telecom Indicators* (1Q15)

Vendor Motivation

"It is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own self-interest." As Adam Smith observed in *The Wealth of Nations* in 1776, his dinner was not being provided as a charitable offering. Likewise, information technology vendors are not charitable institutions and are motivated by their own self-interest, most notably:

- New revenue
- Contractual obligations
- Reputation
- Loss of revenue

The level and extent to which each of these incentives motivate any particular vendor depends on the specific circumstances. Vendors are highly incentivized when pursuing new customers and new revenue. In these situations, they will go far to win new business, offering great introductory discounts, simplified license models, and hard-to-meet service-level promises all to acquire the customer and the associated revenue. This applies to all technology segments: telecommunications, hardware, software, and services. Likewise, after the contract is signed, vendors are highly incentivized to meet contractual obligations as legal disputes are a costly detractor from their core business operations. Furthermore, repeated failures to support customer needs are often highlighted by industry analysts in their reviews. Vendors work hard to make sure their failures don't make the headlines. Again, with all these

incentives along with the freedom of choice, why do vendors fail to live up to their customers' expectations?

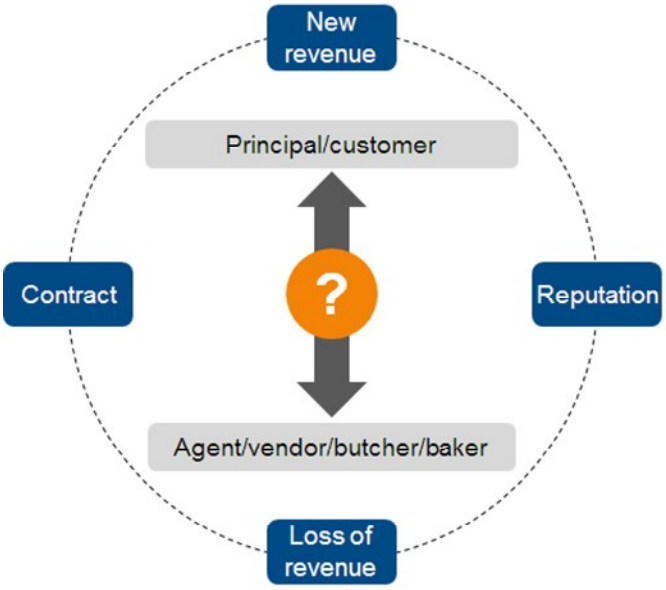
Key Assumptions

First, we assume that we are dealing with existing vendors under a current contract not in pursuit of new customers/revenue. Second, negotiating effective contracts with service-level agreements (SLAs) that provide the right incentives to vendors for achieving certain outcomes is truly a daunting task. For the purpose of this research study, we assume that a contract document, frozen in time, cannot provide all the right incentives in an extremely complex and amorphous technology outsourcing environment. With that said, IDC advises all enterprises to maintain rigorous SLAs that address all aspects of the vendor's delivery model to help ensure the contract continues to provide as much incentive as possible throughout the duration of the term of the contract. And finally, we assume that every failure to meet every business need will not result in a loss of reputation.

Figure 2 highlights the incentives motivating vendors.

FIGURE 2

Vendor Motivation



Source: IDC, 2015

Control Points Limit Freedom of Choice

With three of the four noted incentives neutralized, the only remaining incentive that keeps vendors meeting the expectations of their customers is the potential loss of revenue when the contract governing the relationship expires or is terminated. If an enterprise is not happy with the level of service provided by the vendor, unless there is a significant cost to replace the vendor and related technology, the enterprise is free to choose to find an alternative. Nevertheless, all too often, high

switching costs or other control points such as proprietary technology integrations, make the prospect of finding an alternative vendor or technology economically unjustifiable.

Nevertheless, for some vendors, the threat of nonrenewal is enough of an incentive to promote the correct behavior and to keep the best interests of the enterprise in the forefront. In such cases, the threat of a nonrenewal or termination is real. However, all too often, the vendors have the upper hand: the technology or service provided is so highly integrated into the infrastructure, processes, and business operations of the principal customer that the threat of nonrenewal or termination is a remote and distant possibility, switching costs are far too prohibitive, and the customer is no longer free to choose. The result is vendor lock-in.

For example, take a 2nd Platform database technology deployment at a typical large enterprise. After a decade and millions of man-hours integrating enterprise-class applications with a single proprietary relational database management system, it is no longer feasible for an enterprise to switch database vendors without incurring enormous switching expenses. And why, some may ask, is this an issue? After all, there is a reason why the enterprise standardized on the best technology available at the time. The database management system was scalable, dependable, fast, and secure, with well-documented APIs and an extensive toolset. From a technical perspective, there is no better solution. All is well until a license model change drastically increases the maintenance costs for enterprises using the proprietary technology. Did the enterprise consider these risks as it diligently worked to standardize on the database technology and customize its application? It is IDC's observation that the standardization on such proprietary technology during the early years of the 2nd Platform was more often the result of "herd behavior" than well-thought-out decisions.

By now, most are familiar with the stereotypical, overly customized enterprise application that has taken decades to modify, adapt, customize, and integrate (see Figure 3) – so much so, that the underlying code can no longer be upgraded and switching to another application vendor is not feasible without incurring the time and costs of customization again. Although the practice of over-customization is much less frequent that it was over a decade ago, it is still worth mentioning so that the same mistakes made implementing 2nd Platform technologies should not be repeated with 3rd Platform technology.

FIGURE 3

Customization Lock-In

Source: IDC, 2015

As a more contemporary example using a 3rd Platform technology, a start-up in the social media market segment uses a proprietary cloud platform as a service (PaaS) to quickly ramp up its business. The APIs, services, and development tools made available by the PaaS vendor decrease time to market and help the venture develop applications and grow quickly. If successful, the venture will find itself locked-in with no easy way out of the proprietary PaaS. Conversely, without using the chosen PaaS, the venture may not have the resources to develop the application or the lengthy development cycle may prevent the venture from capitalizing on a small window of opportunity as competitors launch their own solutions. Similarly, large enterprises eager to cut development time and expense are attracted to such platforms. And, if the benefits outweigh the risks, leveraging such a platform will provide great business value, helping enterprises move forward with digital transformations necessary to help compete in the changing marketplace.

Open Source

The VSMO should be careful not to overlook lock-in considerations even in areas with "open" standards and technologies. As another example, during the 1980s, a new business model was introduced by the information technology ecosystem – open source software. At the core of the open source model were loosely knit communities developing open source software profiting only on the support revenue provided to open source users. Customers were free to use the open source software and free to choose any vendor for support.

Over time, the open source content of major open source vendor technology stack distributions has been overshadowed by proprietary ancillary code, which is necessary to manage the open source content. Although vendors may standardize on the same open source version or kernel, switching from one vendor's fully loaded stack to another is no longer feasible for a large enterprise without a significant effort. What was once open is now closed and is a potential vendor lock-in situation.

SaaS/Cloud

It may help to think of a cloud environment as an operating system. Applications can developed to run on a particular operating system. Porting them to operate on another is a significant effort. Similarly, an enterprise can spend a lot of time and effort moving its applications to a particular cloud environment. Porting them to another cloud environment is a big effort, especially after years of adding additional workload and applications. Accordingly, standardizing on a cloud environment is a serious decision that has long-term financial implications for an enterprise.

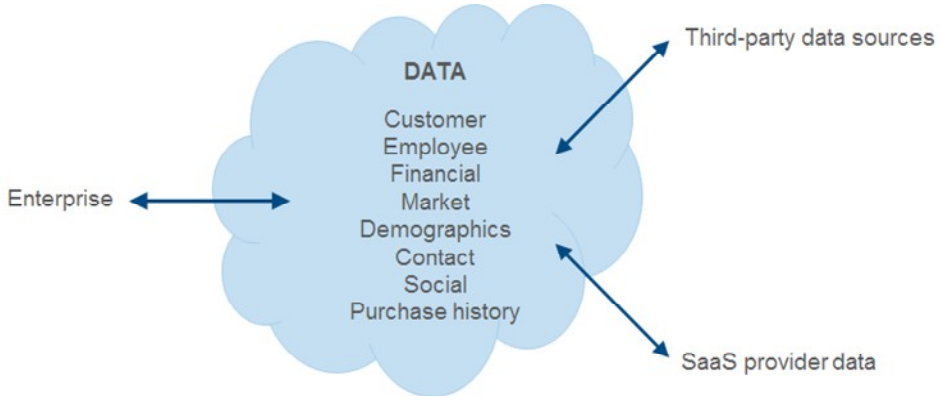
Even in the SaaS market segment, contrary to conventional wisdom and logic, vendor lock-in is a significant concern. Certainly, in the case of SaaS it is easy to terminate a service from one vendor and start service with another. Nevertheless, migrating business data and information stored in one system to another is a project requiring extensive resources from the enterprise, and both new and old vendors. Assuming that the terminated vendor is contractually required to provide the data, migrating may be of questionable use without significant cooperation and resources provided by the vendor. If the data is maintained in a proprietary database architecture, a conversion effort will be required, and, unless the appropriate cooperation is obtained, the project may prove more costly and take longer than forecast. Of course, if the SaaS provider does not provide a mechanism to extract the data provided by an enterprise during the use of the SaaS, an enterprise may find itself in a position of starting over from a point in time prior to its relationships with the incumbent SaaS provider.

Furthermore, the ownership of the data necessary to operate the application in the cloud may provide another vendor control point. Many SaaS providers provide integration points with proprietary data sources: sales leads, contact information, financial information, market data, demographics, and so forth (see Figure 4). While the enterprise may retrieve, store, and benefit from the data provided, what, if anything, can the enterprise do with the data after the contract is terminated. Whose data is it? After all, didn't the enterprise pay a fee for the data? Perhaps the fee just covered the temporary use in the context and confines of the SaaS. If not clearly addressed in a contract, the question of what an enterprise can do with the data outside of the context of the SaaS may be one for a legal professional, and, subject to opposing legal opinions.

IDC has predicted that by 2017, 35% of vendor sourcing relationships around 3rd Platform technologies will fail. Given those concerns, combined with security, legal, and other issues, 3rd Platform initiatives accelerate the need for IT due diligence in the procurement of IT services (see *IDC FutureScape: Worldwide CIO Agenda 2015 Predictions,* IDC #252235, October 2014). Accordingly, enterprises must apply the requisite due diligence when selecting their cloud and SaaS providers, or risk being locked-in to a vendor and/or technology that has failed to deliver the desired outcome.

FIGURE 4

Who Owns the Data?



Source: IDC, 2015

Maintaining Positive Relationships with Locked-In Vendors

Now, let us make an assumption that an enterprise determines to assume the risks associated with embracing a proprietary technology and pursues the benefit of a faster time to market, an improvement in business performance, or just a general decrease in short-term cost. In other words, we will assume an enterprise has made a conscious decision to lock-in to a particular vendor. There have been many sound business cases made to support such decisions. In such a situation, many performance concerns may be addressed by ensuring there is a complete and thorough service-level agreement and associated contract in place that protects the interests of the enterprise. However, as mentioned previously, it is virtually impossible to address every potential concern that may come along, especially in the context of the quickly changing 3rd Platform. In such situations, it is imperative that an enterprise maintain positive relationships with these key vendors that will be leading them through the digital transformation.

Accordingly, the enterprise should consider establishing relationships at all appropriate levels, commensurate with the importance of the technology being leveraged. For example, after implementing and standardizing on a new SaaS-based customer relationship management solution, the appropriate leadership from the enterprise (CIO, CMO, COO, and staff) should continue to nurture and maintain positive relationships with their peers at the vendor. The enterprise is less likely to be caught by surprise with respect to changes in technology road maps, licensing models, data ownership, price increases, and other issues. Furthermore, vendors are far more likely to address service or quality issues with enterprises that behave as collaborative partners.

Similarly, it is important to thoroughly investigate previously established relationships and reputation of the potential vendor/partner. Enlist the support of your network within and outside of the enterprise. For example, IDC maintains an extensive knowledge base of enterprise/vendor interactions and experiences. Partnering with a vendor having a long history of unfairly leveraging control points to extract maximum revenue from its customers may be a risk not worth taking, despite a compelling technology platform. Accordingly, vendors that developed a reputation of leveraging control points as they developed and marketed solutions for the 2nd Platform will likely continue to do so as the 3rd Platform matures.

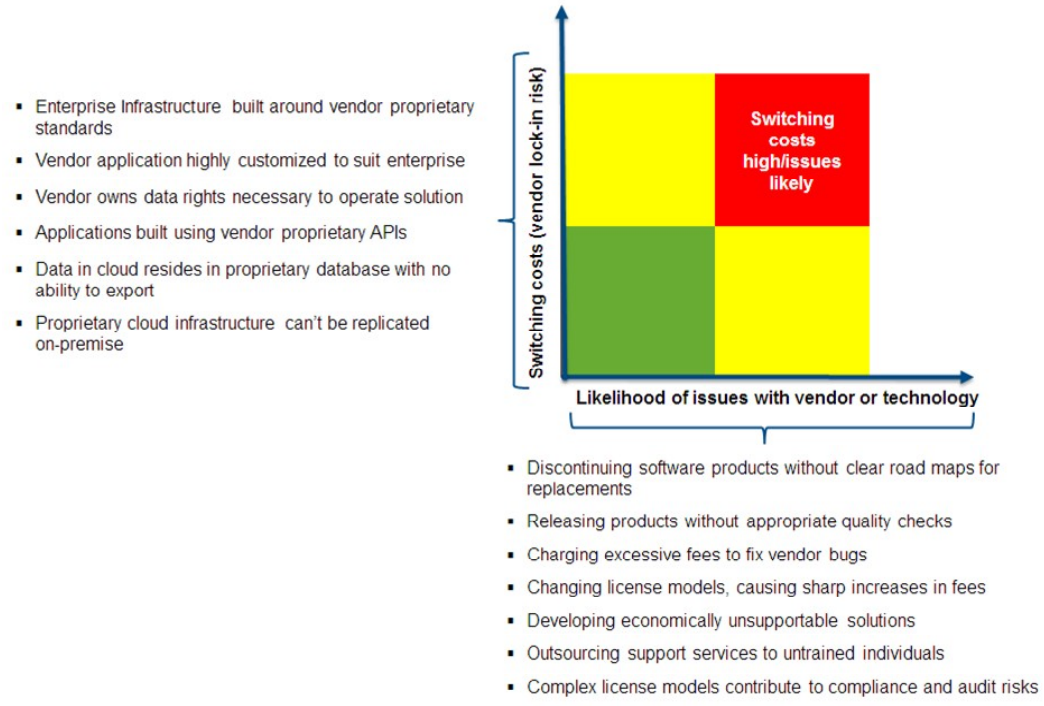
Vendors strategically engineer their solutions to have "control points." After all, why wouldn't they? Making sure that it is easy for customers to migrate away from their technology to competing solutions is not in their best interest. That is, unless potential customers, after reviewing such risks determine that the lock-in risks outweigh the short-term benefits.

Vendor Lock-In Assessments

By conducting audits assessing vendor lock-in vulnerabilities, procurement and IT executives can better understand the financial implications to their enterprises. The enterprise should assess the enterprise technology portfolio and identify key technologies that have a significant impact on the operation of the enterprise (see Figure 5). The vendors and technologies that are most likely to create operational or financial issues should be identified. Furthermore, vendors that have the highest replacement or switching costs (vendors in the upper right-hand quadrant of Figure 5) should be identified and reviewed on a periodic basis. In this manner, the enterprise will be able to better manage its technology portfolio in order to maximize the value it brings to the business.

FIGURE 5

Lock-In Assessment Quadrant



Source: IDC, 2015

In addition, new technology and vendor evaluation criteria should routinely include such assessments. Implementing unique and proprietary features that set one vendor's products apart from the rest may provide benefits from an operational perspective but do such gains outweigh the vendor lock-in risk? By evaluating technology portfolios with vendor lock-in considerations in mind, an enterprise is better able to assess its leverage points heading into major negotiations with vendors. Furthermore, decisions to implement competing technologies in parallel with each other may help create leverage points for the enterprise that help combat the control points set by the vendors. This is the intersection of procurement and information technology that is so critical to the development of strategic business plans that will keep enterprises free to choose and vendors delivering quality products and services.

Lessons Learned for a VSMO

As mentioned previously, it is IDC's observation that vendor lock-in considerations were rarely a factor in making technology and vendor decisions when the 2nd Platform was nascent but growing at a fast pace. The rapid growth of technology quickly outpaced an enterprise's ability to understand such risks. Enterprises were leaving the 1st Platform (mainframe) behind in droves. Decisions were being made by technologists eager to implement the latest and greatest technology to harness the power and flexibility of decentralized computing and of the Internet – the herd outpaced an enterprise's ability to govern.

VSMOs, if present in an enterprise, did not have the experience or foresight to look at the negative aspects of embracing a proprietary technology. Only after the 2nd Platform had matured did such concepts and considerations become apparent. Of course, by then it was too late. Many enterprises had completed their ERP implementations and customizations and proprietary network and database integrations.

As the adoption of the 3rd Platform begins to reach the same pace encountered during the rise of the 2nd Platform, VSMOs should learn from the lessons of the past: they must carefully consider vendor lock-in considerations and engineer their vendor strategies and implementations to avoid lock-in situations. If the decision-making authority is rightfully vested in an organization that considers all aspects of a vendor and technology selection and procurement effort, making decisions based on a herd mentality will be minimized.

FUTURE OUTLOOK

The 3rd Platform is quickly growing and taking hold in the IT ecosystem. IDC has predicted that by 2018, one-third of the top 20 market leaders in most industries will be significantly disrupted by new competitors that use the 3rd Platform to create new services and business models (see *IDC Predictions 2014: Battles for Dominance – and Survival – on the 3rd Platform,* IDC #244606, December 2013). Accordingly, the digital transformation will make the 3rd Platform a key differentiator for enterprises willing to embrace it and make it a key element of their business model, product, or service. Nevertheless, as previously mentioned, IDC predicts that by 2017 over one-third of all vendor relationships around 3rd Platform technologies will fail. Furthermore, according to Aaron Polikaitis, vice president of IDC's IT Executive Programs (IEP), Vendor Sourcing and Management practice, "An even greater percentage of all enterprises with 3rd Platform vendor relationships will continue limping along in these failed relationships because they are locked-in to these vendors." Accordingly, enterprises must apply the requisite due diligence when selecting their cloud and SaaS providers, or risk being locked-in to a vendor and/or technology that has failed to deliver the desired outcome.

ESSENTIAL GUIDANCE

Over the years and decades, enterprises have made tremendous investments in money and resources implementing 2nd Platform technologies used to operate and grow their businesses. Some of the technologies are relatively easy to replace. Others would require a significant investment and/or key business process redesign. In many cases, the costs to replace far outweigh the benefits – the enterprises are locked in to the vendor and/or technology. As enterprises evaluate 3rd Platform technologies, the long-term implications of standardizing on a particular technology or vendor should be thoroughly evaluated. Accordingly, enterprises should:

- **Within the next 6 months:**
  - Identify the 3rd Platform technology evaluations and implementations taking place within the enterprise.
  - Prioritize those technologies that have a strong probability of being adopted by a broad user base.
  - Research the broader long-term implications of standardizing on such technologies.

- **In the short term (6–18 months):**
  - Assess the switching costs for 3rd Platform technologies being implemented within the enterprise by reviewing alternative technologies and vendors.
- **In the long term (beyond 18 months):**
  - Minimize the potential disruption caused by the technologies mentioned in the upper right-hand red quadrant of Figure 5 by reducing, to the extent possible, the enterprise's reliance on them. Add architectural separations in implementation strategies. Curtail plans to expand the reach and footprint of these technologies. Prepare for their replacement.
  - Pay special attention to those vendors that are locked-in to the enterprise architecture. Make sure the appropriate relationships exist between the enterprise and the vendor leadership structure.

LEARN MORE

Related Research

- *IDC MaturityScape Benchmark: Leadership Digital Transformation in the United States* (IDC #256394, June 2015)
- *IDC MaturityScape: Leadership Digital Transformation* (IDC #255709, May 2015)
- *Infrastructure and Cloud Services: Develop a Cloud Exit Strategy Before Signing a Contract* (IDC #252169, October 2014)
- *IDC FutureScape: Worldwide CIO Agenda 2015 Predictions* (IDC #252235, October 2014)
- *IDC Predictions 2014: Battles for Dominance – and Survival – on the 3rd Platform* (IDC #244606, December 2013)

Synopsis

This IDC study provides guidance to procurement and IT executives struggling to manage the most common pitfalls encountered in their relationships with external suppliers. It provides key strategies for minimizing negative behaviors common to outsourcing suppliers. Furthermore, this study guides vendor sourcing and management organizations (VSMOs) in making strategic plans for new relationships with vendors providing 3rd Platform technology solutions. These plans will help the enterprise avoid making technology and vendor decisions in pursuit of short-term gains without appropriately assessing the negative long-term implications of such decisions. Although 3rd Platform technologies and delivery methods have changed, the study applies lessons learned from vendor relationships formed for 2nd Platform technology solutions to key 3rd Platform technology procurement considerations. Maintaining leverage in a vendor/customer relationship is critical to ensure a vendor is motivated to act in the best interest of its customer.

Aaron Polikaitis, vice president of IDC's IT Executive Programs (IEP), Vendor Sourcing and Management practice, notes, "Vendor lock-in eliminates a primary factor motivating vendors to continue delivering in the best interest of the customer."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2015 IDC. Reproduction is forbidden unless authorized. All rights reserved.