Four Tips for Controlling IT's Tail Spend

By **CIO Insight Staff** August 27, 2013 ✧ Updated on: May 12, 2021

By Mark Ball

For most IT organizations, the classic 80/20 rule applies to the supplier portfolio, where more than 80 percent of the total spend is dedicated to less than 20 percent of the organization's total number of suppliers. This is expected because large IT infrastructure systems and resources are typically procured through a relatively small number of well-established IT providers. But problems can arise when IT organizations have a very large number of "tail" suppliers—e.g., small IT suppliers that collectively make up less than 20 percent of the total IT spend. Some large IT organizations might have hundreds or even thousands of such tail suppliers. An excessive number of tail suppliers can create problems in at least three ways:

1. The cost of managing a tail supplier, including onboarding, vendor management, risk management, payment processing and other practices, is often the same as, or

even greater than, managing a larger and more strategic supplier. When this operational expense is multiplied by the large number of suppliers at the tail of the IT spend, the total operational burden can be significant.

2. There is inherent risk in maintaining a supplier portfolio that includes a large number of small suppliers. This should be intuitive, because the more suppliers that are granted access to the company's data, systems, hardware and other resources, the greater the opportunity for breaches in security, system failures, or other risk issues.

3. By spreading the IT costs across a large number of suppliers, the company is not taking sufficient advantage of scale economies and pricing discounts that could be achieved by consolidating its base of suppliers.

It should be noted that this is not an argument against procuring goods and services from small businesses. On the contrary, small, niche IT companies often provide higher quality, lower priced, and unique products and services that larger companies do not offer. The danger lies in maintaining an excessive number of tail suppliers, which prevents the company from efficiently managing a best-in-class supplier portfolio.

Here are four tips for controlling the quantity of tail suppliers:

- **Measure and monitor the tail spend.** As usual, the first step toward a solution is to understand the nature of the problem. It is best to leverage a spend analysis tool that extracts data directly from the company's financial systems in order to determine the size and scope of the tail spend. While organizations may have different definitions of what qualifies as "tail spend," typical criteria might include supplier spend that falls below the dollar threshold of requiring senior management approval and suppliers comprising the bottom 20 percent of the total supplier spend. Robust spend analysis will highlight key metrics such as the number of tail suppliers, the size of the tail spend, the categories and sub-categories most affected, and the business units responsible for driving the tail spend.

· **Define and publish the list of preferred suppliers.** Unauthorized tail suppliers often exist because business managers seek urgent and inexpensive suppliers to satisfy pressing needs. But often the manager is not aware that an existing qualified supplier is already under contract with well-negotiated pricing and terms. The organization should define and communicate a comprehensive yet limited list of preferred suppliers that represent the pre-approved providers for each spend category and sub-category. Within the technology category, the IT organization should identify the core list of staffing firms, consulting companies, support providers, hardware, software and other IT suppliers that represent the organization's preferred list of approved vendors. It is important that the preferred supplier list include an appropriate spectrum of large and small companies, multi-service and niche players, as well as market leaders and low-cost alternatives.

Previous article
Risk-Based Security Management Needs Improvement

Next article
Senior Leadership Needed to Drive Digital Success

CIO Insight Staff

Latest Articles

Why Do Good Workers Leave Bad Managers During a Pandemic?

Careers **Kent Barnett** - August 20, 2021

Hiring Crunch Hits IT

Blogs **Drew Robb** - August 20, 2021

The Future of IT Is Hybrid: Four Tips for CIOs to Find Success

Blogs **Michael Ringman** - August 18, 2021

Related Articles

Can You Pass the Elevator Test? The Importance of Being Likable

Shelby Hiter - August 13, 2021

Is Biometric Technology Worth the Cost?

Lauren Hansen - July 30, 2021

AI Software Trends for 2021

Shelby Hiter - July 29, 2021

What is an Advanced Persistent Threat (APT) Attack?

Shelby Hiter - July 28, 2021

CIO insight

CIO Insight offers thought leadership and best practices in the IT security and management industry while providing expert recommendations on software solutions for IT leaders. It is the trusted resource for security professionals who need to maintain regulatory compliance for their teams and organizations. CIO Insight is an ideal website for IT decision makers, systems integrators and administrators, and IT managers to stay informed about emerging technologies, software developments and trends in the IT security and management industry.

Menu

- IT Management
- IT Strategy
- News & Trends
- Blogs
- Case Studies
- Books for CIOs

Our Brands

Privacy Policy Terms About Contact Advertise California – Do Not Sell My Information