How to Effectively Evaluate an IT Contract

From job contracts to bank loan agreements, CFMs spend countless hours and dollars reviewing contracts and each has its own set of evaluation criteria.

Technology contracts are no different: They often contain specific terms that are helpful and terms to watch for during the evaluation process. While technology contracts may not require as much due diligence as a job contract, contractors should ensure the terms are favorable since company data or operations are often at stake.

Almost every common technology product or service requires a contract, including enterprise resource planning (ERP) systems, cloud hosting, software product licenses, Building Information Modeling (BIM), Customer Relationship Management (CRM) systems, networks, threat prevention software (e.g., virus software, firewalls), technology support, phone systems, mobile devices, Computer Maintenance Management Systems (CMMS), and scheduling systems.

But this list only represents a fraction of available technology solutions. With the increase of technology’s role in business, the quantity and complexity of such contracts will continue to grow.

What sets a technology contract apart from other agreements? Let’s look at an ERP contract as an example. The ERP is one of the most important systems to a company. It contains a wealth of data: job cost, payables, payroll, HR, general ledger, and financials. The accessibility, availability, and security of such data as well as the systems that contain the data are unique to technology contracts.

This article will focus on what questions contractors should ask around these three key areas and will provide tips for negotiating price before entering into a contract with a technology vendor. (Given that each technology vendor has its own unique set of contract terms, the specifics of each type are beyond the scope of this article.)

Data Accessibility

Every technology contract involves data: Some vendors house data, others provide a means to transport data, and others secure the data. Here are some key questions to ask regarding data in the contract language:

- Which party owns the data?
- What type of access does the contractor have to the data?
- What type of access does the vendor have to the data?
- What type of requirements exist for working with and accessing the data?
- Which party can modify the data?
- How can the data be modified?
- In what format is the data stored?

These types of questions are mostly applicable to software that creates or houses data; they are not as relevant for contracts that move or secure data (e.g., network provider or firewall contracts).

Let’s use the previous example of purchasing an ERP to review data accessibility-related items in a contract. Be sure to ask about the infrastructure that houses the data. If the data resides in a proprietary database, then issues with sharing and integrating the data with other software may arise. Along the same lines, ensure the contract language states that the data stored in the system belongs to the contractor, and that the vendor may not obtain or use the data for its own purposes.

A contractor should also determine if it can directly access the database or if indirect data access is the only option. If the contractor has direct access to the database, then custom reports and integrations can occur, allowing for automation and process streamlining. However, if the contractor does not have direct database access, then it would not be able to create automations and custom reports without first exporting the data, which requires extra time and resources.
**Availability**

The next big area of focus for technology contracts is availability. The questions to ask around this topic can apply to almost every technology contract:

- What type of uptime guarantees exist to access the data?
- Does the vendor respond to issues timely?
- What type of redundancy is in place to create the availability needed for the business if the primary system fails?
- What type of testing procedures exist for updates before they go live?
- How crucial is the system to the company's operations?
- Are proper penalties in place to incentivize the vendor to quickly resolve problems?

Let’s return to the ERP software example. Since this ERP software is cloud-based and the system is critical to the contractor, availability is key. Make sure that the contract states the uptime guarantee for cloud and ERP software access. Part of the uptime guarantee will rely on what type of redundancy and backup procedures are in place for the cloud environment. Make sure the contract clearly outlines financial repercussions for downtime as well as the vendor’s testing procedure for updates related to uptime guarantees.

To further understand the importance of uptime guarantees, let’s use a network provider contract as a second example. The main goal of a network provider is to guarantee network bandwidth and access to a customer; here, availability terms must be addressed, including:

- Penalties to the provider for downtime;
- The type of redundancy in place if the primary network connection fails; and
- A specific response time guarantee for downtime. While this item may be difficult to obtain depending on the size of the network provider, it can help quickly resolve problems if it’s included in the contract.

**Security**

Like availability, security applies to any type of technology contract. Given that security is paramount in everything related to technology and likely to become even more important in the future with the continued rise in cyberattacks, consider the following questions:

- Who is liable for damages incurred from a security breach?
- Does the vendor carry proper insurance to cover damages from a security breach?
- What is the regular patch schedule for security updates, and who is responsible for performing the patches?
- What is the vendor’s threat response plan?
- How and in what time frame is the vendor required to communicate security threats or issues to the customer?
- Is there a contingency plan in place by the vendor for security breaches?

Continuing with the ERP example, if an ERP vendor is providing cloud access to software, then security is paramount. Let’s suppose someone were to hack into the contractor’s ERP, successfully steal customer data, and then ask for a large sum of money for the data to be returned.

Why did the cloud provider not detect and notify the company of the hack? Depending on how the contract is written, the vendor may not be responsible for threat detection and notification.

How did the breach occur and who is liable for the damages? If an employee of the contractor created the breach, is the cloud provider removed from liability? Is there an issue of negligence by either party?

Finally, if the cloud vendor is responsible for the breach, does it have proper insurance coverage to protect against the liability? The cloud vendor may be liable, but if it does not have enough insurance, then the contractor may end up covering damages.

Security is crucial to keeping company data safe; considerable time and effort should be spent on this part of the contract. A data breach can quickly become a legal battle if proper terms are not worked out in the initial contract.

**Pricing Terms**

Along with these vital areas, a contractor should closely examine the pricing structure for all aspects of the agreement. Be sure to ask:

- For how long is the price locked in to buy a license at the current rate?
- What percentage can the vendor increase cost and in what time frame?
- Which party handles build-out cost?
- Is the labor quote an estimate or fixed rate?
Let’s revisit the ERP contract example. Even if this ERP has a per-license cost, do not assume this current rate will apply to future license needs. For example, if the current cost of a license is $10,000 and another license is needed in three years, then the cost could increase to $15,000 per license by that time. Try to work in a clause to lock in the current license purchase rate for a set period of time.

Also, watch out for line items that allow the vendor to increase the percentage of the maintenance fee on a contract each year. Try to negotiate a fixed maintenance fee percentage over a period of time, and try to prevent that rate from increasing above a certain percentage.

Certain technology, such as the components needed to create a network, will often have a build-out cost. For example, if the contractor is trying to set up a network far from the provider’s point of origin, then the provider may try to pass a build-out fee directly to the contractor or conceal it in the monthly rate of the contract. Try to reduce or eliminate this fee if possible.

Finally, consider if the contract involves labor from the vendor. If a fixed labor amount or limit is not given, it is another area that can add extra cost.

**Conclusion**

With so many provisions to consider, how can a contractor negotiate on these terms, obtain the right price, and maintain a good relationship with the vendor? The key is to gain an understanding of what is being quoted and how each item of the contract impacts your company. Decide which items are must-haves and which can be negotiated. Then, work with the vendor to modify the contract accordingly. The vendor will understand what contract items can and cannot be changed and will likely be flexible on some items.

Do not be afraid to ask questions. The more knowledgeable you are about the system, the better you’ll be able to talk with vendors without getting lost in the technology jargon. This is especially the case with multiple systems contracts and master service agreements. (See the sidebar at right.)

Along those lines, CFMA’s Connection Café is a great way to post questions and obtain feedback. And, for a deep dive into key technology terms, check out “How to Talk Tech to Get Business Results” by Dennis J. Stejskal in the July/August 2015 issue. With so many items to watch out for in contracts, knowing what you are talking about is key.

As long as a contractor focuses on the main areas of data, availability, and security while watching out for the potential gotchas, it’s possible to negotiate a technology contract that works for both the contractor and the vendor.

---

JASON KEEN, CCIFP, is Corporate Controller with Lehman-Roberts Company, a heavy/highway contractor in Memphis, TN. With a background in technology and systems implementations, Jason’s areas of expertise include reporting, analysis, system implementations, vendor relations, contract negotiation, and process improvement.

A member of CFMA, Jason participates on several committees, including the Financial Survey & Benchmarking Committee and the Heavy/Highway Subcommittee.

Phone: 901-774-4000, ext. 127
E-Mail: jkeen@lehmanroberts.com
Twitter Handle: @thejasonkeen

DAVID MIDDLETON is the IT Manager at Lehman-Roberts Company, a heavy/highway contractor in Memphis, TN.

While attending the University of Memphis David interned at the Lehman-Roberts Company in the IT department. He is a graduate of University of Memphis, where he received a BBA in Management Information Systems.

Phone: 901-774-4000, ext. 169
E-Mail: dmiddleton@lehmanroberts.com
Website: www.lehmanroberts.com

---

**Master Service Agreements**

Master service agreements act as overarching terms for multiple system contracts with one vendor. For example, if your ERP company also provides cloud services and another type of software, all three will be governed by a master service agreement. If not automatically provided, the contractor may have to request this agreement from the vendor and review it before signing the contract.

If you buy a new piece of software or a new license from a vendor and already have a master service agreement in place, be sure that the new contract does not trigger a revision of the master service agreement. The contract may contain a clause that could render addendums the contractor made on the original master service agreement null and void.