DoD ESI White Paper

Best Practices for Negotiating Cloud-Based Software Contracts

Guidance on the differences between purchasing perpetual software and renting Software as a Service

About DoD ESI

The DoD ESI was formed in 1998 by Chief Information Officers at the DoD. To save time and money on commercial software, a joint team of experts was formed to consolidate requirements and negotiate with commercial software companies, resulting in a unified contracting and vendor management strategy across the entire department. Today, DoD ESI's mission extends across the entire commercial IT life-cycle to include IT hardware products and services. DoD ESI has established DoD-wide agreements for thousands of products and services.

www.esi.mil

Executive Summary

As the utilization of cloud computing grows within the Information Technology (IT) arena, it is challenging organizations to think differently about IT procurement. This paper addresses the key contractual concepts to focus on when negotiating a public cloud, Software-as-a-Service (SaaS) delivery model versus a traditional on-premises software delivery model. Under both models, use rights are still granted, but there are variations of the software use terms and conditions, especially in areas such as licensing and costs.

From an overall contractual perspective, most terms and conditions remain the same between a traditional on-premises software perpetual licensing contract and a SaaS contract, since the same software and functionality are being supplied by the software provider. However, there are differences, such as Grant of a Software License and Payment Terms.

When deciding to use a SaaS provider, the focus shifts from buying, implementing and managing the software application to establishing and managing the SaaS vendor relationship. The SaaS Subscription Agreement and Service Level Agreement (SLA) are critical for a successful relationship to deliver all anticipated benefits. All aspects of the relationship need to be negotiated upfront, including:

- Ability to request customizations, enhancements, data base queries, new reports – and the negotiated costs
- Ownership of any software customizations or enhancements
- Data rights and responsibilities throughout data lifecycles
- Information security and confidentiality
- Cost and pricing metrics
- Additional user provisioning and usage metering
- Uptime and performance guarantees
- Issue response and resolution times
- Maintenance and support, including system administration, application of patches, fixes, and upgrades
- Disaster recovery and business continuity
- Contract termination conditions

Knowing what to include in your contracts with SaaS providers will both maximize and protect your organization's cloud investments.

Table of Contents

Cloud Computing Introduction and Background 4

Why Organizations Move to the Cloud 6

Contract Differences: "Traditional" Delivery Model versus the Cloud 7

Rights to Use the Software 7

Payment Terms 8

Key Points When Negotiating a SaaS Contract 9

Underlying SaaS Agreement 9

SaaS Service Level Agreement (SLA) 11

Conclusion 13

Cloud Computing Introduction and Background

The term "cloud computing" is becoming mainstream in the IT world and has been gaining momentum within recent years. Some believe that the concept of cloud computing has been around since the beginning of the IT outsourcing industry in the 1960s when Ross Perot rented idle computing power from one company to carry out the processing needs of another (mostly during the night). The company that owned the computers monetized its down time, and the organization that needed the computing power did not have to outlay capital for equipment, thus creating a win-win situation.[1] This bartering of computing power would soon become a commodity, made possible via the Internet (the cloud) and would not only focus on using idle computing power, but now also, creating computing power for the sole purpose of providing a service to another company.

As the utilization of cloud computing is increasing, its definition is expanding too. A broad definition is that cloud computing is the scalable provisioning of IT as a service using the Internet or a network. Some of the IT capabilities contributing to scalability and elasticity include virtualization and service-oriented architecture, which have helped to create various cloud models. The three main cloud computing models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS):

- **IaaS** is a provisioning model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.
- **PaaS** is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. It adds vendor management of the operating system, middleware and runtime data base to the IaaS offering. PaaS is often used by developers to build applications on top of the computing infrastructure. This might include developer tools that are offered as a service to build services, or data access and database services, or billing services. [2]
- **SaaS**—"In a pure SaaS model, the provider delivers software based on a single set of common code and data definitions that are consumed in a one-to-many model by all contracted organizations anytime, on a pay-for-use basis, or as a subscription based on use metrics."[3] It essentially adds data management and application management to a PaaS environment. All you have to do is connect via the Internet and use it. Some software vendors are now offering or are thinking of offering some form of SaaS model to deliver their software. SaaS is being adopted in multiple industries, such as Customer Relationship Management (CRM), human resources for talent acquisition and procurement.

In addition to the three cloud models identified above, clouds can also be private, community, public or hybrid:

- **Private Cloud** is operated solely for a single organization, whether managed internally or by a third-party and hosted on or off premises.[4] Private clouds are usually virtualized cloud data centers inside an organization's firewall, or they may be a private space dedicated to an organization within a cloud provider's data center. [5] Nevertheless, in private cloud computing, access to the cloud is limited to internal users. Also, in private cloud computing, users still have to purchase the internal hardware and software, implement and manage the solution and thus do not benefit from lower upfront capital costs and less hands-on management. Of course, these costs can still be mitigated somewhat by creating more efficient environments through virtualization – or by taking the off premises route to private clouds by asking the vendor to provide dedicated resources for critical data or applications.

- **Community cloud** is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public Cloud** is the delivery of cloud services (e.g. software applications) over the Internet by a third-party provider to the general public. It exists on the premises of the cloud provider and usually includes virtualization for more efficient deployment of shared resources.
- **Hybrid Cloud** is any combination of external public cloud services and internal resources to create a solution. "Hybrid cloud computing implies significant integration or coordination between the internal and external environments. Hybrid cloud computing can take a number of forms, including cloud bursting, where an application is dynamically extended from a private cloud platform to an external public cloud service, based on the need for additional resources."[6] It may exist on or off premises. In the completely off-premises hybrid model, a provider can supply a shared virtual environment along with private, dedicated, data storage space all on the provider's premises.

For the purpose of this paper, "cloud" is used to refer to the architecture setup of how software is delivered as a service via the Internet (SaaS via a public cloud). Under this delivery model, software is hosted by the software provider or a third party hosting provider off-premises from a user's facilities. This paper addresses the key contractual concepts to focus on when negotiating a public cloud SaaS delivery model versus a traditional on-premises software delivery model. Under both models, software use rights are still granted, but there are variations of licensing terms and conditions, especially in areas such as usage rights and licensing costs.

Interestingly, shortly before the publication of this paper, The National Defense Authorization Act for Fiscal Year 2012 (H.R. 1540) changed the DoD's November 2011 statement regarding a "DISA First" approach to Cloud Computing. Section 2867, subsection b, paragraphs 2B (ii) II through IV of this bill stipulates a Department-wide strategy for:

"(II) Transitioning to cloud computing.

(III) Migration of Defense data and government-provided services from Department-owned and operated data centers to cloud computing services generally available within the private sector that provide a better capability at a lower cost with the same or greater degree of security.

(IV) Utilization of private sector-managed security services for data centers and cloud computing."[7]

In response to the 2012 NDAA, DoD cloud computing strategies and policies will address use of commercial cloud services. This is further evidence that cloud computing is a significant topic for DoD.

It is clear that cloud computing is becoming mainstream. This is evident when nonprofit organizations such as the Open Networking Foundation (ONF) are being created. ONF was formed in March 2011 by Deutsche Telekom, Facebook, Google, Microsoft, Verizon, and Yahoo!, ONF hopes to promote a new approach to networking called Software-Defined Networking (SDN). SDN hopes to create technology standards that can be leveraged for cloud computing purposes by creating the switching mechanism to support the OpenFlow interface. OpenFlow enables networks to evolve by giving a remote controller the power to modify the behavior of network devices, through a well-defined "forwarding instruction set." This growing OpenFlow frontier includes routers, switches, virtual switches, and access points from a range of providers.[8]

Cloud computing advances via OpenFlow and other new emerging technologies are examples of the shift that organizations will need to make in order to align their resource requirements to manage cloud providers. Skill sets for these roles will include individuals with strong IT vendor management and quasi-technical skills. These resources will serve as critical liaisons between IT, the business and the cloud provider.

Why Organizations Move to the Cloud

The number of organizations currently leveraging or thinking about leveraging the cloud continues to grow. The following statistics are indicative of reported trends:

28% of US organizations are using cloud computing.[9]

21% average annual savings for applications moved to the cloud.[10]

By year-end 2016, more than 50% of Global 1000 companies will have stored customer-sensitive data in the public cloud.[11]

The following paragraphs list the most common benefits for choosing a cloud delivery model over a traditional delivery model.

Cost Reduction: The government's plan to migrate large amounts of IT services and IT assets to the cloud is expected to help the government save millions of dollars and reduce its infrastructure footprint by more than a third by 2015.[12]

By choosing a cloud delivery model for your needs, you save the cost of building and maintaining your own infrastructure to run the software, just as Ross Perot's customers did many years ago. Since "renting" the right to use software as a service can be less expensive in the short term than buying a perpetual software license outright, you save money on the cost of the initial investment by only paying for what you actually use and not paying for what you may use in the future. Therefore, your total cost of ownership (TCO) may be reduced depending on the discounted upfront costs, lower operational costs by not having to implement and maintain software in-house, and other benefits realized by choosing a cloud delivery model.

Note: See Appendix 1 for a basic costing model to compare various deployment models. A detailed examination of cost-benefit will be provided in a future White Paper.

However, it is important to mention that each organization's specific use scenario should be analyzed on an individual basis. Whether or not a cloud delivery model offers a cost avoidance over perpetual software in the long run must be determined. The cost analysis will differ depending on an organization's preferred return-on-investment (ROI) timeframe (e.g. 3 year ROI vs. 5 year ROI, etc.) and TCO determinants.

Speed and Flexibility: Many of today's information technology teams are plagued by having too few resources to keep up with constantly evolving internal demands. With cloud computing, organizations are realizing the benefit of having flexible solutions, where they can scale the software service up and down as needed within a much quicker timeframe. The initial deployment of software via the cloud or adding more users to an existing SaaS delivery model can be faster and less expensive than traditional non-cloud models due to the reduction of complex procurement and deployment cycles (e.g. not needing to obtain and install a new license key for additional users). Additionally, many SaaS providers include self-service provisioning for adding functionality and new users.

Greater Connectivity and Mobility: By using cloud services, you can access your software and inherent data from any device that has access to the Internet (assuming your chosen software also has a mobile device interface or native application).

Heightened Security: Leading cloud providers often have cutting-edge, secure, and traceable data access trails.[13] Most cloud servers will be hosted in physically secure data centers with strict access control for their own staff and no access for unauthorized personnel. At the same time, it is interesting to note that 43% of CFOs whose organizations are implementing hybrid and private clouds are less than "somewhat open" to moving business-critical applications into those environments, because they are concerned with reliability, security, availability and performance.[14] Overall, cloud service providers can provide heightened security, but it is important to confirm where and how your information is being stored to ensure you are really achieving a greater level of security.

Easier Collaboration and Integration: Cloud computing provides quicker speeds in which we can interact with each other and more efficient ways for completing collaborative tasks. SaaS opens up the Internet to be used for more than obtaining research information or checking email. SaaS providers are now creating pre-established application programming interfaces with popular applications that their services interact with for many of their clients. This collaborative approach for sharing information and driving business results is the way of the future. "The push to deliver information, websites and web-based application functionality as composable Web services is a key catalyst that is driving the delivery of "everything as a service." [15]

Contract Differences: "Traditional" Delivery Model versus the Cloud

From solely an overall contractual perspective, most terms and conditions remain the same between a traditional on-premises perpetual licensing contract and a SaaS contract (e.g Limitation of Liability, Indemnification, etc.), since the same software and functionality are being supplied by the software provider. However, a few key differences are Grant of a Software License and Payment Terms.

Rights to Use the Software

Within the cloud delivery model, software use rights are subscription-based (you are renting the right to use the software as a service for a specific term). You pay on a monthly or annual basis for usage. This subscription fee or cost includes right to use the software, plus any software assurance/maintenance which is provided by the cloud service provider.

For a traditional software purchase, the right to use the software is normally purchased in perpetuity (you are buying a license to use the software forever). You pay one lump sum upfront and, depending on the software, maintenance fees for technical support and functionality upgrades. (The buyer gets basic warranty service for a specific period of time. Additional support beyond the warranty must be separately purchased under a separate software assurance or maintenance agreement.)

It is important to understand that sometimes traditional on-premises software is also provided via a subscription or finite term where you do not own the right to use the software in perpetuity.

Perpetual Licensing: The perpetual licensing model is more common for traditional on-premises software. When purchasing the right to use software in perpetuity, the full license rights may depend upon how payment terms are structured. Additionally, you may not own all of the code, since the software provider may only allow you to modify, if at all, only a particular layer of the code (object code vs. source code). This licensing model is not offered as an option for public cloud SaaS delivery models. Whether or not this licensing model would be readily utilized for a private or hybrid cloud delivery model is yet to be seen (depending on the ability to move existing applications into a private cloud instance).

Subscription Use: The subscription model only allows the right to use the software service while the subscription is valid (i.e. paid up-to-date). This is the most common model for public cloud solutions. This grant of usage model may be possible for hybrid cloud solutions where you can negotiate terms such as:

- Pay a maximum subscription fee over a specific term and then you have the right to use the software in perpetuity or have the option to use in perpetuity for an incremental pre-negotiated licensing fee; or
- Break out the hosting fees versus the software licensing fees so the two are not intermingled.

Payment Terms

The payment terms between the cloud and a traditional software delivery model can vary greatly. The most pronounced difference is that under a traditional model you may be able to withhold a portion of the software license fees until after the Go-Live Date or Acceptance Date of your software product. Additionally, you may defer maintenance payments until after the Go-Live date.

Alternatively, cloud-based solutions sometimes bundle together hosting, software licensing/use rights and maintenance fees into one monthly or annual fee. Thus, you are required to start paying for the service as soon as you authorize the cloud provider to turn it on, even though you may not be using it in production yet. For instance, you may need time to setup data integration or implement other items such as single sign-on capabilities, but the SaaS provider may still charge full usage price. Therefore, be careful to only commit to the number of users that you need upfront and ramp up your usage thereafter as demand warrants.

To mitigate this practice by SaaS providers (making your organization pay for software before your users even have a chance to login into the system), see if the SaaS provider has a sandbox or proof-of-concept environment where your associates can become familiar with the software at little to no charge before signing a contract for a specific term and number of users.

Key Points When Negotiating a SaaS Contract

When organizations move to a public cloud delivery model, it's like an outsourcing engagement to a certain degree, where you rely upon the management and expertise of another party. In order to help build trust with an organization considering outsourcing, Ross Perot would remind them that his company was the IT expert by stating, "You are familiar with designing, manufacturing and selling furniture, but we're familiar with managing information technology. We can sell you the information technology you need..."[16] Feeling comfortable that a SaaS provider is the expert in hosting your data and managing your software application takes time. SaaS is relatively young compared to conventional outsourcing arrangements, but there are transferable concepts that can be leveraged.

Much like a conventional outsourcing engagement, when deciding to use a SaaS provider, your organization is no longer focusing on managing the technical software application. Instead, it must shift its attention to managing the SaaS vendor relationship. This is where heavy IT contract negotiation, contract management and vendor management skills come into play. All rights and responsibilities that are associated with the relationship should be memorialized in an enforceable contract and effectively managed until the relationship has been terminated.[17]

The specific risks to be addressed in your contract with a SaaS provider will depend upon a number of factors:

- The application you are using (e.g. what use purpose does it support?)
- How critical the application is to your business to help determine the necessary availability levels that will be demanded (e.g. is it customer facing and/or does it provide a key business function?)
- The data that will be exchanged, stored and maintained by the SaaS provider (e.g. how sensitive is the data, where will it will be stored and who will have access to it?)

These risks can be mitigated by careful review of the SaaS provider's system setup and by the terms and conditions of your SaaS contract.

The remainder of this section will cover the key negotiating points for two critical contract areas: the underlying SaaS Agreement and the Service Level Agreement (SLA). These paragraphs assume that standard software licensing terms will be included in the contract, such as intellectual property rights, indemnification, limitation of liability, warranty and cure period, etc.

Underlying SaaS Agreement

- Ensure that the right to use the software is clear and that there are no hidden fees. For example, if the pricing metric for the service is determined by the number of users, is the metric per unique/seat users, concurrent, or only active users? Does the provider also charge for technical support users who are not really using the software application, but need ad hoc access to it?
- Clearly identify all of the functionality you are paying for from the provider to ensure they do not degrade this functionality over time. One good way to memorialize this in the contract is to attach a functionality matrix with screenshots of the software application as an appendix to the contract. Also, be sure to list all additional and optional fees in the contract, such as additional storage fees, custom reports, etc.

Ownership of Customizations or Enhancements

- Clearly identify who owns any customizations or enhancements, especially if your organization pays for them as "work product" developed solely for your organization (e.g. an individual branch of the provider's standard base code that is unique to your organization and for which you paid for the development effort).

Data Rights and Responsibilities

- Include language that states who owns data during all of its lifecycle, including when data is transferred or exchanged (data in transit) and during storage (data at rest).
- Aso include language regarding who bears the risk for loss of data in transit. Depending on the nature of your data and how it is processed, you may need to negotiate language to affirm your organization's ownership of the results of any processing of its data that occurs on the cloud provider's systems.[18]
- Define and confirm a process with your provider that allows for regular backup of your data on your premises. This safeguard is important as SaaS providers can, in fact, lose data.[19] However, the need for on-premises data backup is situational, depending on the criticality and comfort level of your organization with each SaaS engagement. Possibly no on-premises backup is needed, but this should be considered. Contracts cannot totally safeguard against the risk of data loss, but they can offer additional layers of protection related to your data rights within the cloud.
- Define what the provider's responsibilities are in the event of 1) a security breach (e.g. ensure they provide an immediate notice if your data may be compromised); 2) an outage; and 3) termination (e.g. ensure the provider will cooperate with the return of your data in a format and manner previously agreed, and with no additional fees for the return of data).

Heightened Confidentiality, Security and Disaster Recovery

- Confidentiality language is found in all contracts, but SaaS contracts should contain heightened confidentiality language relative to the DoD and the Federal Information Security Management Act (FISMA).
- Obtain detailed information about the service provider's security processes and procedures, including data flow diagrams. One way to obtain this information is to leverage a questionnaire approach. The Cloud Security Alliance's Consensus Assessments Initiative Questionnaire serves as one good example that can be leveraged to build your own questionnaire.[20] Draft these minimum security conditions into the contract and obligate the provider to maintain them throughout the term of the agreement.
- Ensure that the DoD is involved in reviewing and determining what data will be stored by the provider and what layers of security need to be in place. This includes making sure all applicable Information Assurance (IA) Policy and regulatory documentation is made part of the agreement reference list.
- Confirm how data access will be limited, including review of the different user permission roles offered, the various accessibility parameters for each role, and the administrator's access rights (e.g. ensure all users' actions can be tracked).
- Ensure your organization has the right to audit the provider's facilities and documentation to verify that minimum security levels are in place and being enforced, including confirmation that your data is located where it should be and not being sent to a third party or being intermingled with other clients' data.
- Ask for third-party reports regarding penetration and vulnerability results for provider's hosting environment.

- Include language confirming what the provider's data storage period and data destruction policy are.
- Include language confirming the provider's business continuity plan, specifying redundancy requirements to include, at a minimum, data backup and recovery methods/infrastructure/processes. Also, have the provider certify that they will participate with you in disaster recovery testing at specific time intervals (e.g. once every two years) without charge.

Termination

- Even though providers may lock your organization in for a specific contract term and minimum number of users, ensure the ability to terminate for cause, including a continued lack of uptime—specific criteria should be identified in the SLA (see "SaaS Service Level Agreements" below).
- Ensure payment terms are clear and confirm that the provider cannot immediately shut off services for late or disputed invoices.

SaaS Service Level Agreement (SLA)

The key components of any solid SLA should contain specific, measurable and enforceable terms and conditions that the SaaS provider must adhere to for each component of the service provided. If the provider fails to meet an obligation under the SLA, the SLA must have the "teeth" to help mitigate such failure from happening again. The "teeth" to SLAs are the specific remedies that apply when the provider's obligations are not met. The remedies usually take the form of monetary damages that are pre-agreed between the parties for specific failures and/or credits for future services.

The key components to include in a SaaS SLA, as described in the following paragraphs, are contact information, issue response and resolution times, uptime and data throughput performance guarantees, and maintenance and support.

Key Contact Information

- List all account management and technical support contact information, including mobile phone numbers. This information will change over time, but it is a good practice to include it in the SLA. The information should be reviewed several times during the year to ensure it is up to date.
- Identify the provider's regular hours of operation and support, and identify where their support centers are located. This is useful to know, especially if their support centers are off-shore.
- Ask the provider to define their escalation process and draft it into the SLA, so other persons within your organization will know whom to contact. This helps to provide information to others who will need to carry on vendor management responsibilities after the initial project team.

Response and Resolution Times

- Include a matrix that identifies 1) the priority levels for different software modules and the diverse technical issues that can arise; 2) the provider's response times; and 3) the provider's expected resolution times for each. (Resolution times may not be guaranteed by the provider, but response times should be).
- Have the service provider contractually commit to at least a monthly call or meeting to review service performance, SLA metrics and any service issues. Also, keep an independent "issues" log to match up against the provider's ticketing system in case there are discrepancies.
- Ensure your organization has the final say in determining the severity level for each potential issue.

Uptime and Performance Guarantees

- Identify the guaranteed uptime and application performance metrics needed for each software service component.

- Ensure uptime and performance calculations are listed in the SLA and that they can be objectively and easily measured on a rolling basis (not per calendar month).
- Quantify the downtime allowed in terms of hours or days so you can truly understand the impact of downtime business needs. (For example, a 99.7% uptime would mean that there is approximately 11 allowable days of unplanned downtime in one year. A recommended approach would be to negotiate at least a 99.9% uptime, allowing for less than four days of downtime in one year.)

  NOTE: Even if organizations are willing to pay extra for an extremely secure environment with a guaranteed 100% uptime, it may be cost prohibitive and just not possible.
- Hold the provider accountable for things within their control. For instance, a SaaS provider cannot control the public network, the Internet, but they should be able to provide you with reports regarding the time it takes your data to be processed and actionable steps on their side for the specific service you are using affected by unplanned downtime. Also, they can share risk with their counterparts and ensure that the network providers they choose also have contingency plans in place to ensure uptime.
- Identify the provider's standard maintenance windows.
- Define what "planned maintenance" means and confirm that the provider will provide at least 48 hours' notice for downtime to be considered "planned maintenance."
- Define the calculations to be used for credits if uptime or application performance guarantees are not met. An example of an uptime formula is the following (this is not meant to be a suggested formula to be used, but only as an example).

Service Level Uptime:

- Service Level is 99.96%.
- Uptime Percentage is calculated for any rolling 30 calendar days as follows:

$$\text{Uptime Percentage} = \frac{\begin{array}{c}\text{Total number of}\\ \text{expected uptime}\\ \text{minutes}\\ \text{in any 30 days}\end{array} \quad \textbf{Minus} \quad \begin{array}{c}\text{Total number}\\ \text{of minutes of}\\ \text{unplanned downtime}\\ \text{in any 30 days}\end{array}}{\begin{array}{c}\text{Total number of expected}\\ \text{uptime minutes in a given 30 days}\end{array}}$$

Service Credits: Should the Service Level fall below 99.96% for any consecutive 30 day period, the service provider will provide a credit (based upon the applicable month's charges for the period in which the Service Level failed) as noted in the chart below:

Uptime Percentage	Credit
< 99.96%	**50%**
< 99.90%	**75%**
< 99.50%	**100%**

- Explain the process to obtain a credit, including the notice period needed for requesting the compensation and when and how the compensation will be provided.
- Confirm what type of software application service monitoring and alerts are available. Some providers now have websites that publish this information on an ongoing basis.
- Include the ability to terminate the entire agreement without further liability if uptime fails over a particular period of time (e.g. if uptime

drops x amount over x number of rolling days). Most cloud providers will want you to commit to at least a year of service (usually paid monthly). However, what if you sign a one-year deal and the service is down for five days straight upon the start date? Do you still want to be committed to that provider for the next 360 days?

Maintenance and Custom Support

- Identify how many major and minor versions of the software are allowable compared to the provider's most recent generally available (GA) version.
- Ask about the frequency of releases and upgrades (both minor and major) upgrades upfront. Codify the notification process for releases and ensure that you can opt out of releases or upgrades (assuming that your instance is not too many versions behind their most recent generally available version).
- Identify the ongoing support expectations for any customizations and enhancements. This includes identification of turnaround times if custom reports that you cannot create on your own are needed (e.g. reports that require the provider's help or third-party professional services).

Conclusion

Today, cloud computing is another new approach to solving persistent, old IT problems, such as doing more with less, providing ultimate flexibility at very low cost and being first to market with new products. Just as the initial concerns and resistance to off-shoring gave way to intelligently governed outsourcing models, a similar trend will emerge on the cloud front.[21]

One of the key challenges for cloud computing customers is to ensure contracts include the provisions needed to guarantee appropriate use rights, services, resource availability, infrastructure capability, security, system and environment support, maintenance, SLAs and other matters important to your end users and their mission.

Today's buyers of these services now have to be proficient not only in matching technology to requirements, but also managing contracts and vendor relationships. Skill sets for these roles will include individuals with strong IT vendor management and quasi-technical skills. These resources will serve as critical liaisons between IT, the business and the cloud provider. They will have to ensure that cloud contracts include language that is easily understood and enforceable while not "over contracting". They will also need to ensure that expected savings and efficiencies are actually achieved.

About the Author

Gretchen Kwashnik currently serves as the IT Supplier Management Team Leader at ING DIRECT, USA in Wilmington, DE. Her responsibilities include technology acquisition, IT contract management, IT supplier management, and the integration and management of IT project contractors. Gretchen began her ING DIRECT career in the Procurement department, drafting and negotiating IT and Marketing contracts. In 2008, she transitioned to the IT department, where she has since concentrated on technology acquisition, the software development life cycle, and the facilitation of IT projects. Gretchen has a Bachelor of Science in International Business from King's College and a Juris Doctorate from Widener University Law School.

Appendix 1 – Costing Model for Cloud versus Traditional Models

	Perpetual On-Premises Model	Perpetual Hosted Model	Subscription PaaS Model	SaaS Model
Applications				
Data				
Runtime				
Middleware				
O/S				
Virtualization				
Servers				
Storage				
Networking				
Application Personnel				
Data base Admin				
Networking Engineers				
Hardware Engineers				

[1] Article, “Cloud Computing–Been There, Done That” by Raj G. Asava. Found at: http://www.perotsystems.com/CountrySites/UnitedKingdom/MediaRoom/WhitePapers/Cloud_Computing.

[2] Book, “Cloud Computing For Dummies” by Judith Hurwitz, Robin Bloor, Marcia Kaufman, Fern Halper.” Published November 16, 2009 by Wiley Publishing, Inc. Excerpts found at: http://www.dummies.com/how-to/content/cloud-computing-cheat-sheet.html.

[3] Article, “Key Issues for Software as a Service, 2011“by Robert P. Desisto and Ben Pring. Published March 24, 2011 by Gartner, Inc.

[4] Article, “The NIST Definition of Cloud Computing“ by Peter Mell and Timothy Grance. Published September 2011 by the National Institute of Science and Technology (Special Publication 800-145).

[5] Book, “Cloud Computing For Dummies” by Judith Hurwitz, Robin Bloor, Marcia Kaufman, Fern Halper.” Published November 16, 2009 by Wiley Publishing, Inc. Excerpts found at: http://www.dummies.com/how-to/content/cloud-computing-cheat-sheet.html.

[6] Article, “Key Issues for Cloud Computing, 2011” by David Mitchell Smith. Published April 1, 2011 by Gartner, Inc.

[7] National Defense Authorization Act for Fiscal Year 2012, H.R. 1540, 112th Congress of the United States

[8] Open Networking Foundation’s website and press release on March 21, 2011 found at: https://www.opennetworking.org/about (as of September 24, 2011).

[9] CDW 2011 CLOUD COMPUTING TRACKING POLL

[10] CDW 2011 CLOUD COMPUTING TRACKING POLL

[11] Article, “Gartner’s Top Predictions for IT Organizations and Users, 2012 and Beyond: Control Slips Away” excerpt by Gavin Tay. Published November 23, 2011 by Gartner, Inc.

[12] Article, “Amazon cloud crash endangers federal websites” by Joseph Marks. Published on April 21, 2011 by National Journal Group, Inc. Found at: http://www.nextgov.com/nextgov/ng_20110421_7729.php.

[13] Article, “The Healthcare Cloud Confusion: 3 Reasons Why You Should or Shouldn’t Adopt the Cloud” by Karin Ratchinsky. Published on September 8, 2011 by Level 3 Communications’ “Beyond Bandwidth” blog. Found at: http://blog.level3.com/2011/09/08/the-healthcare-cloud-confusion-3-reasons-why-you-should-shouldnt-adopt-the-cloud/.

[14] Symnatec’s 2011 Virtualization and Evolution to the Cloud Survey. Found at: https://www4.symantec.com/mktginfo/whitepaper/Virt_and_Evolution_Cloud_Survey_060811.pdf.

[15] Article, “Key Issues for Cloud Computing, 2011” by David Mitchell Smith. Published April 1, 2011 by Gartner, Inc.

[16] Article, “Tips to Make An Outsourcing Project Successful.” Published on April 23, 2011 by Outsourcing Smartly. Found at: http://outsourcingsmartly.com/tag/ross-perot/.

[17] See Wikipedia, Cloud Computing, http://en.wikipedia.org/wiki/Cloud_computing (describing the history and application of Cloud Computing) (as of September 24, 2011).

[18] Article, “If It’s in the Cloud, Get It on Paper: Cloud Computing Contract Issues” by Thomas J. Trappler. Published in EDUCAUSE Quarterly Magazine, Volume 33, Number 2, 2010. Found at: http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/IfItsintheCloudGetItonPaperClo/206532.

[19] *Article, “Amazon’s cloud crash destroyed many customers’ data” by Henry Blodget. Found at: http://technolog.msnbc.msn.com/_news/2011/04/28/6549775- amazons-cloud-crash-destroyed-many-customers-data (as of September 24, 2011).*

[20] Article, “Open source fuels growth of cloud computing, software-as-a-service” by Jon Brodkin. Published July 28, 2008 by Network World, Inc. Found at: http://www.networkworld.com/news/2008/072808-open-source-cloud-computing.html.

[21] Article, “Cloud Computing–Been There, Done That” by Raj G. Asava. Found at: http://www.perotsystems.com/CountrySites/UnitedKingdom/MediaRoom/WhitePapers/Cloud_Computing.

DoD ESI is an official
Department of Defense initiative
sponsored by the Department of Defense
Chief Information Officer (DoD CIO).

**Your Preferred Source for
IT Acquisition Across the DoD**

BEST VALUE

EFFICIENT

LOW RISK

VOLUME DISCOUNTS

UNIFIED VOICE

Visit DoD ESI online at **www.esi.mil**

Department of Defense Chief Information Officer
6000 Pentagon
Washington, DC 20350-6000