Gartner Global IT Councils

A Gartner Global IT Council brings together IT leaders to discuss a chronic challenge and develop a common approach to solving it. Gartner facilitates and moderates the council, but the council’s findings represent the council’s views, not necessarily those of Gartner. The council discusses the issues that matter most to members and offers the solutions that members believe will work best for them. Council meetings encourage open discussion that will result in real-world recommendations and drive fundamental changes in the way the IT industry works. The document produced by the council represents the collective voice of some of the IT industry’s most influential, thoughtful and forward-thinking leaders.

Gartner has established two Global IT Councils—one on cloud services and one on IT maintenance. A core component of the council concept is the belief that improvements in industry practices will benefit not only IT customers and clients, but also developers, vendors and other stakeholders.

Each of the Global IT Councils has been tasked with developing a set of basic rights and/or responsibilities for their specific area of technology. Members have discussed the issues candidly and in depth, and offered their real-world observations about problems in these areas, as well as practical, actionable recommendations for resolving them.
Rights and Responsibilities for Consumers of Cloud Computing Services

A computing paradigm such as cloud computing carries risks that are slowing corporate adoption. For example, cloud providers serving thousands to millions of customers generally cannot tailor contracts to address the individual needs of a given customer. Tailoring each contract makes it difficult to scale such a business model. Thus, most public cloud services operate the same way for all customers with only minor differences. This "commoditization" of service delivery introduces risks to service consumers, who may have little power when a provider fails to deliver what is promised. To minimize these risks, service providers and service consumers must agree on a set of shared objectives and expectations.

All service consumers should have some basic rights to protect their interests. If cloud services are commoditized, providers should offer stronger customer guarantees. However, service providers either do not offer protections or vary greatly in the protections they do offer across areas such as ownership of data, service-level agreements and technical requirements. In addition, service providers and service consumers share responsibilities for the relationship, and each side must take action to achieve proper business outcomes.

Accordingly, the Gartner Global IT Council for Cloud Services has defined six rights and one responsibility of service consumers that will help both providers and consumers establish and maintain successful business relationships. This document describes some of the most pressing rights and responsibilities along with the reasons why they are necessary. Additional critical rights and responsibilities will emerge as cloud services mature.

To determine what the rights of service consumers should be, Gartner convened an IT council comprising CIOs of large enterprises that consume cloud services. The council members met over four months in the first half of 2010 to discuss the most pressing issues affecting cloud computing today, and they summarized their views in the six rights and one responsibility of cloud service consumers. As the industry addresses these issues, other issues requiring further statements may come to the fore. For now, the council urges its peers to insist that providers acknowledge and respond to these rights and responsibilities.

The council’s discussions focused primarily on enterprise use of the public cloud and the issues that might drive enterprises to a more private offering. The emergence of general-public providers in the cloud challenges enterprises that need guarantees of service performance. General-public providers of cloud services deliver generalized services to massive numbers of customers for economies of scale, so the business model prevents these providers from offering service consumers customized treatment. Enterprise-public providers, which serve perhaps dozens to hundreds of customers, have a little more scope for working with customers individually, but their business still requires them to standardize more than, say, application service providers. This document does not address enterprise-private cloud providers, which provide services only to the enterprises that sponsor them.

Rights and Responsibilities of Cloud Service Consumers

1. The right to retain ownership, use and control of one’s own data
2. The right to service-level agreements that address liabilities, remediation and business outcomes
3. The right to notification and choice about changes that affect the service consumer’s business processes
4. The right to understand the technical limitations or requirements of the service up front
5. The right to understand the legal requirements of jurisdictions in which the provider operates
6. The right to know what security processes the provider follows
7. The responsibility to understand and adhere to software license requirements
In early 2010, Gartner conducted a field survey of 300+ users of cloud computing. Among other questions, respondents were asked to rank their top 3 drivers for adopting cloud computing and their top 3 concerns when adopting cloud computing. The findings appear below in tabulated form. We hope they provide useful context for readers of this report.

### Top drivers for adopting cloud computing

<table>
<thead>
<tr>
<th>Driver</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meet security requirements and data location/privacy requirements</td>
<td>30%</td>
</tr>
<tr>
<td>Ability to grow or shrink usage and pay only for consumption</td>
<td>25%</td>
</tr>
<tr>
<td>Cost or ease to deploy the cloud service</td>
<td>20%</td>
</tr>
<tr>
<td>Meet service-level and/or support requirements</td>
<td>15%</td>
</tr>
<tr>
<td>Speed or ease to obtain required functionality</td>
<td>10%</td>
</tr>
<tr>
<td>Avoid or reduce upfront capital investment</td>
<td>10%</td>
</tr>
<tr>
<td>Cost or ease to customize the cloud service</td>
<td>10%</td>
</tr>
<tr>
<td>Cost or ease to integrate cloud service with existing systems/apps</td>
<td>10%</td>
</tr>
<tr>
<td>Pay-as-you-go financial model</td>
<td>10%</td>
</tr>
<tr>
<td>Supplier credentials (reputation, financial strength, references)</td>
<td>10%</td>
</tr>
<tr>
<td>Business expansion or contraction</td>
<td>10%</td>
</tr>
<tr>
<td>Avoid operations or administration responsibilities</td>
<td>10%</td>
</tr>
<tr>
<td>Unable to expand existing data center facilities</td>
<td>10%</td>
</tr>
<tr>
<td>Other</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: Gartner Field Survey, January – February 2010 (n=332, top 3 choices)

### Top concerns when adopting cloud computing

<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security of service</td>
<td>40%</td>
</tr>
<tr>
<td>Data location, privacy or access concerns</td>
<td>25%</td>
</tr>
<tr>
<td>Perceived loss of control or choice of technology</td>
<td>20%</td>
</tr>
<tr>
<td>Cost uncertainty or variability</td>
<td>15%</td>
</tr>
<tr>
<td>Increased business risk</td>
<td>10%</td>
</tr>
<tr>
<td>Dealing with compliance with regulations</td>
<td>10%</td>
</tr>
<tr>
<td>Inadequate service levels (e.g., availability, performance)</td>
<td>10%</td>
</tr>
<tr>
<td>Lack of industry standards</td>
<td>10%</td>
</tr>
<tr>
<td>Lack of awareness of confidence in model</td>
<td>10%</td>
</tr>
<tr>
<td>Lack of suppliers with satisfactory credentials or reputation</td>
<td>10%</td>
</tr>
<tr>
<td>Inadequate contract terms or termination arrangements</td>
<td>10%</td>
</tr>
<tr>
<td>Other</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: Gartner Field Survey, January – February 2010 (n=332, top 3 choices)
Rights and Responsibilities of Cloud Service Consumers

The council resolved to recognize six rights and one responsibility that pertain to consumers of cloud computing services.

1. The right to retain ownership, use and control of one’s own data

The Problem: Many cloud service providers do not explicitly state their position on the issues of ownership, use and control of data. When a service provider hosts data, processes and applications on behalf of a service consumer, does the provider now gain the right to use, access or manipulate those resources without the permission of the service consumer? The common-sense answer is certainly not. However, without a statement from the provider to this effect, there is a potential risk to the service consumer.

Providers also vary in the rights they do allow service consumers. This variation and lack of clarity lead many enterprises that could benefit from cloud services to choose alternative delivery models. Enterprises that use cloud services may run into unexpected problems accessing or controlling their data, for example, if their service provider is acquired or goes out of business. In outsourcing deals, the enterprise can solve this problem by spelling out terms in the contract; the general-public cloud model does not allow enough flexibility for this solution.

The Council’s View: The council agreed that service consumers should retain ownership of, and rights to use, their own data. The issue is clear-cut when only the service provider accesses the service consumer’s data. It becomes more complicated when multiple parties access the data, such as in a business-to-business service in which suppliers and customers access the data as well as the service provider.

The council insisted on the importance of data security in the issue of ownership and control. Several members support enterprises (for example, a national security organization, an insurance company and a media company) and projects where protecting client data and intellectual property is paramount. Regulators oversee this protection in financial services and other industries. The projects include a public cloud service that would enable all public agencies in a U.S. state to exchange information, and a high-performance grid that would allow universities and national security agencies to communicate. Members’ use of the term “security” encompassed many different issues:

- **Protection.** The service provider must safeguard the service consumer’s data both when it resides in a database or repository and while in transport over networks.

- **Clearance.** The provider must guarantee that data does not sit in its systems after the service consumer ceases to use it, and that no unauthorized party accesses the data while it’s being cleared.

- **Access.** The service provider must authenticate users and provide appropriate levels of access control. However, the service consumer must retain ownership and control over users’ IDs.

- **Encryption.** Some large service providers do not want to encrypt subsets of data. They want all of the data encrypted or none of it because they cannot customize encryption for every customer.

- **Staff.** The provider must explain how it monitors and controls access by staff. The provider must set policies regarding which of its employees can see the service consumer’s data and under what circumstances. The provider must also follow good hiring practices, including background checks, so that the staff is trustworthy.
The security aspects spill over into questions about use and control. The service consumer must retain the right to approve any disclosure of data for legal or compliance purposes. The provider must also specify what it can do with the consumer’s data—for example, would the provider use the service consumer’s customer data to support its own CRM efforts? Lack of clarity on this point can lead to costly legal battles. In 2007, for instance, a woman sued Virgin Mobile for using a photo of her daughter in an ad. Virgin Mobile obtained the photo from Flickr, and the woman did not understand what rights she was giving up when she posted it there. The parties settled out of court.

Finally, consumers could lose control of their data when their service providers go out of business or are sold to other companies. The original contract or service-level agreement must provide for the clear disposition of the service consumer’s data in case the provider can no longer provide service. Data recovery, transfer of data to an alternate provider, and secure deletion of the consumer’s data from provider systems should all be addressed.

Providers will have to supply some level of assurance about consumer data, or enterprises will hesitate to put significant portions of their business in the cloud—particularly enterprises in regulated industries. In many cases, the legal department will prevent deals that would otherwise happen. The challenge of providing these assurances will only increase because many different countries, even governments at the state and provincial levels, will enact their own data protection laws. For example, California, Massachusetts and New Hampshire have recently done so in the U.S. German law forbids enterprises from sending data about German employees out of the country.

Initially, service providers and consumers will work out these issues primarily in contracts. Over time, practices around data protection will become codified in standards overseen by industry organizations.

Resolved: The council unanimously agreed that service providers must do the following to uphold this right:

- Furnish an audit statement of data ownership and usage practices.
- Provide an audit statement of the minimum relevant data management certifications, which will vary according to industry. For example, enterprises doing business with the U.S. government must comply with U.S. laws such as the Federal Information Security Management Act.
- State their policy and procedures for e-discovery, including the circumstances under which they will divulge information owned by the consumer.
- Disclose the location, movement and usage assumptions about data and applications delivered as part of the cloud service but owned by the service consumer.
- In contracts, specify remediation for failing to adhere to stated policies and standards related to data ownership, use, privacy and accessibility.

2. The right to service-level agreements that address liabilities, remediation and business outcomes

The Problem: All computing services suffer slowdowns and failures, including cloud services. However, cloud service providers seldom commit to recovery times, specify the forms of remediation or spell out the procedures they will follow. Moreover, providers that do offer these kinds of guarantees do so only for their own environment. (Although the overall performance of the service—which is what matters to the consumer—also depends on the network connecting provider and consumer and on the consumer’s own systems.) Service-level agreements often describe commitments in technical terms, such as throughput and uptime, but these don’t necessarily make sense for the consumer’s business.
The Council’s View: The key observation made by council members is that cloud services require different kinds of service-level agreements, depending on the type of service provided. When the business uses internal services, it often contracts with the IT organization for storage, CPUs or application uptime. These measures may make sense for cloud infrastructure services. But when the business turns to cloud providers for applications, it wants to buy outcomes—customers served, units delivered, transactions processed and so on. Therefore, the cloud provider should write service-level agreements that directly relate to the business outcomes sought by the service consumer.

To make service-level agreements relevant to the business, providers do not have to customize them for every consumer; rather, the agreements should comprehensively address the business issues implied in the type of service offered. For example, suppose a service consumer runs an application that consumes a certain amount of CPUs. The consumer then introduces a new offering, which causes traffic on its website to shoot up. The provider’s contract should not simply guarantee a certain turnaround time for adding capacity; it should specify how it will deliver that capacity, including:

- The provider’s technology, technical limits and technical requirements (so that the service consumer knows what is feasible)
- The procedures by which the capacity will be added (what triggers the additional capacity, where it will come from and so on)
- Pricing (for example, a congestion pricing plan)

Service-level agreements covering service outages might detail plans for local failover or remote disaster recovery. In addition to quick recovery, a service consumer’s business will need remediation of any problems caused by the outage. For example, the provider may recover lost data, but if the consumer cannot identify which entities a transaction involved or what workflow was executing when the outage occurred, the consumer cannot reconstruct the transaction and complete its business with the customer.

The performance of the service end to end poses a challenge because it depends on systems outside the immediate control of the provider. For the consumer, it would make sense to craft service-level agreements that involve all parties, including the service provider, the network provider and the service consumer itself. If a database or application that consumers in Michigan access from a provider in Phoenix, Arizona, runs slow, it does not help the consumer to hear that it’s not the provider’s fault.

The consumer needs to measure the service’s performance end to end, although this measurement may be possible only for enterprise-public cloud providers, not the big, general-public providers. Monitoring performance may entail looking at message traffic, violations, security rules and other indicators. The consumer may already have monitoring tools that it uses internally; the provider may supply such tools, or third parties can monitor service performance. Naturally, the service consumer must take responsibility for the performance of its own systems—for example, it must allocate disk space properly on local machines to support the service.

The level of guarantee must suit the complexity of the service provided. Simple data backup and restore services can transition easily, for example, but running a payroll in the cloud requires higher levels of control and may call for the provider to place its software code into escrow.
Resolved: The council unanimously agreed that service providers must do the following to uphold this right:

- Write service-level agreements that relate to the business needs of service consumers, not simply address technical issues. For example, a provider that leads consumers to put important parts of the business in the cloud with promises of security must alert the consumer to any compromise within a specified time frame, guarantee no 0-day exploits or set other specific benchmarks above basic security.
- Specify remediation for service or procedure failures that will be meaningful to the service consumer’s business.
- Grant the service consumer access to information about the service to help it assess liabilities and risks.
- Gain the approval of the service consumer for any changes to service-level agreements.

3. The right to notification and choice about changes that affect the service consumer’s business processes

The Problem: Consumers buy services to support their business processes. Once they have signed up with a provider, any change to the terms, such as prices or upgrades, could damage the business because the cost to switch to a different provider is high.

The Council’s View: Every service provider will need to take down its systems, interrupt its services or make other changes in order to increase capacity and otherwise ensure that its infrastructure will serve consumers adequately in the long term. Service providers cannot guarantee that no service disruptions will occur, and must declare whether they allow service consumers to opt out of changes. Instead, protecting the consumer’s business processes entails providing advanced notification of major upgrades or system changes, and granting the consumer some control over when it makes the switch.

Providing adequate notification will still prove a challenge, even to enterprise-public cloud providers, because service consumers differ widely in the data they put in the cloud, the systems they use and even enterprise culture.
The council members acknowledged that not all providers have this level of flexibility, and they anticipated that cloud providers would come in two tiers. The largest providers, such as Amazon and Google, would continue to provide basic, standardized services on a massive scale while smaller providers, with hundreds or a few thousand customers, could provide some customization and process guarantees to support more complex services.

Resolved: The council unanimously agreed that service providers must do the following to uphold this right:

- Provide estimated restore times during service outages, not just for data but for all the elements of the business processes affected by an outage.
- Guarantee notification a specified number of months in advance of any major changes to the service.
- State the requirements for canceling contracts in case outages or changes to the environment force the service consumer to find another provider.
- Explain how they will help the service consumer move data and applications out of the service in the case of a need to migrate or abandon the relationship.

4. The right to understand the technical limitations or requirements of the service up front

The Problem: Service consumers often turn to the cloud to support long-term initiatives. During this time, either the consumer or the provider will inevitably make major changes to its environment, such as data migrations, capacity increases, server upgrades and network changes. Most service providers do not fully explain their own systems, technical requirements and limitations so that after consumers have committed to a cloud service, they run the risk of not being able to adjust to major changes, at least not without a big investment.

The Council’s View: The council members agreed that service consumers and providers must do a better job of keeping each other informed about their technical limitations, particularly for complex, long-term projects or complex architectures and systems. One council CIO cited a problem with transporting data that surfaced late in one project. His enterprise participated in this project along with several others. One of the last steps was to transfer data to the service provider. His own enterprise did not have a problem because it could directly move data to the provider’s server just as in an internal data migration. However, other enterprises did not have a direct connection and discovered that they did not have enough bandwidth to move the data.

There are limits to the technical adjustments that service consumers and providers can make. A provider cannot automatically upgrade an operating system or underlying system components to accommodate new demands from a consumer. Likewise, a consumer should not have to upgrade its own systems to keep up with unexpected upgrades on the provider’s side. In addition, some system changes may be impossible even if the consumer or provider were willing to undertake them. One council member said that his enterprise had contracted with a cloud provider to run a certain software product, which both sides believed was compatible with the provider’s hardware. However, the provider had a more advanced version of the server than the enterprise assumed. The software would not run on the later version, and the provider could not downgrade to an earlier version of the server because it was no longer available.
Cloud services also rely on systems run by third parties. Another council member’s enterprise encountered problems with the network connections between itself and the provider. Neither of them owned the network. The network capacity had to be the right size, but the usage of the cloud service varied greatly from week to week. Too little capacity would hurt the service’s performance. Therefore, someone had to ensure that the network could handle the load. Whose responsibility is it, the service consumer’s or the provider’s?

These examples indicate that providers should set clear policies around major changes, such as price increases, upgrades and patches. Because switching costs are high, contracts should make pricing predictable and not allow for significant jumps (perhaps at most a yearly cost-of-living increase). Providers should also guarantee advance notice of major upgrades so that service consumers have time to plan for the upgrade or make an orderly transition to another provider. Consumers need some flexibility with patches because one approach will not suit everyone. One consumer’s business may demand the security of a rapid patch, and the consumer may be willing to absorb the cost, while the patch might crash another consumer’s systems. One council member recommended using two providers for a given service to guard against unexpected demands or problems with one provider.

Resolved: The council unanimously agreed that service providers must do the following to uphold this right:

- Describe the technical details and limitations of their infrastructure and components before a contract is signed so that the service consumer knows of any changes it must make to use the service properly.
- Indicate the comfortable limits of their systems up to which the consumer would not have to make major investments to expand capacity.
- Inform the consumer of any major system changes a specified number of months in advance so that the consumer can adjust its environment.
- Detail the limits of price increases during the life of the contract.
- State the limits or frequency of major system or architectural changes during the life of the contract, including potential price increases (for enterprise-public cloud providers, which offer more customized or high-value services).
- State their limits of liability resulting from system changes or outages, including any financial penalties they will pay to compensate the service consumer.
- Establish a remediation process for service failures or changes that hurt service consumers, including a way to deal with disputes and problems consumers may have because of the changes.

5. The right to understand the legal requirements of jurisdictions in which the provider operates

The Problem: The ease and speed of deploying and using cloud services also make it easy for service consumers to overlook critical legal issues. If the cloud provider stores the consumer’s data in a foreign country, or transports the data through one, the service consumer becomes subject to laws and regulations it may not know anything about. Service providers have not done a good job of explaining which jurisdictions they put data in and what legal requirements the service consumer must therefore meet. Some providers may not want to say where they locate data for security reasons.

The Council’s View: Legal, political and cultural issues may put data privacy at risk in certain geographical regions or zones. Thus, this right relates to Right No. 1 on data
ownership. The council discussed several situations in which the lack of transparency about where data is can harm the service consumer:

- The CIO of a major cable TV network said that moving intellectual property into a foreign country—for example, to serve up video clips—may violate copyright, a critical issue in the media industry.
- The CIO of a major cosmetics company said that consumer goods companies have to pay attention to the location of data when they market their products. For example, China, Germany and the United Kingdom have rules about where data fed to consumers can come from.
- Transactions that occur in or through a foreign country may make the service consumer liable for taxes in that jurisdiction and obligated to file financial disclosure documents.
- Placing data in a foreign country may make the service consumer subject to anti-terror laws, such as the USA PATRIOT Act, which allow the government to look at the consumer’s information.
- Even transmitting data on a network through another country may make the consumer subject to that country’s laws—for example, if a U.S. service consumer uses a South Korean provider that sends data back and forth over Japanese cables, Japanese law applies.

Thus, the service consumer needs reassurance that the provider does not violate rules in any country and leave the consumer accountable. For example, suppose a provider starts running a service from Germany and then moves it to China—will the provider act as a safe harbor? Alternatively, the service consumer’s business may require it to locate data only in one country or certain countries. The provider may not have facilities in those countries. Amazon, one of the largest cloud providers, has data centers in only three countries.

The lack of guarantees will prevent enterprises from putting their data in the cloud. Amazon and other large general-public providers sometimes provide a dashboard to show consumers where their data is but do not guarantee the data will not be moved. Even this level of assurance won’t be enough for those in regulated industries, those involved with national security and those needing to protect intellectual property rights, such as media companies.

Of course, enterprises will not put all their data in the cloud, but they need to know where a service provider they are considering would put their data so that they can make an informed decision about whether to use cloud services. The council believes that service providers have an opportunity to differentiate themselves from competitors by ensuring that their cloud services do not violate any laws or any agreements the service consumer has made.

Resolved: The council unanimously agreed that service providers must do the following to uphold this right:

- Disclose in which jurisdictions they store and transport the service consumer’s data before signing a contract.
- Discuss any requirements or restrictions that agreements between the service consumer and its customers have placed on the location of data.
- Disclose known impacts when data resides in a given geographical region. For example, providers that house data in the U.S. should disclose in the contract that the data is subject to the USA PATRIOT Act.
• Disclose whether service consumers can specify where data must reside and be notified of changes to the location, and of the legal, political or cultural impact.

6. The right to know what security processes the provider follows

The Problem: With cloud computing, security breaches can happen at multiple levels of technology and use. Service consumers must understand the processes a provider uses so that security at one level (say, the server) does not subvert security at another level (say, the network). Without this knowledge, service consumers risk security violations caused solely by the provider not accounting for the ways in which consumers might use a service. Service consumers also need to understand a provider’s business continuity plans so that they can ensure the continuity of their own operations in an emergency. Service providers are not consistent in explaining either their security processes or their business continuity plans.

The Council’s View: Service providers will only share so much information about their security with consumers. Providers may describe their intrusion detection and prevention systems, for example, and their firewalls. Beyond a certain point, though, revealing too many details becomes a vulnerability for everyone. After all, a provider may serve a thousand consumers, so the odds of sensitive information about the provider’s security getting into the wrong hands multiply enormously. A council member who is CIO for a government entity sympathizes with providers because his enterprise wrestles with the question of how much to reveal to local governments and other states with which it interacts.

Nor can consumers demand that providers use specific security mechanisms, such as a particular access management system. Therefore, the key to this right lies in good communication. The provider must explain its security processes and reliably notify consumers of any potential breaches. However, service consumers must have enough sophistication to understand the implications of these processes for a cloud architecture. Also, many providers shy away from fast, complete notification because they may feel it reveals a lapse on their part; they would rather tell the consumer once the problem has been solved. Unfortunately, this delay leaves the consumer vulnerable.

In addition to security, the provider must explain its business continuity plans and demonstrate that they work, by performing monthly drills, for example. This information will help the service consumer better manage risks and keep its own operations going in an emergency.

Council members had a couple of ideas for ways to increase confidence between service provider and consumer. First, members thought that accounting firms should audit the security practices of providers. To reduce costs, the accounting firms could approach the audits with a common framework (for example, one used by the U.S. Department of Defense). Providers would know what is expected, so the audits would not be onerous. The audits would reduce the level of risk for service consumers.

Second, council members envisioned an independent website where providers could list their certifications, audits, practices and technologies. Prospective consumers could then search to find the provider that best matches their own requirements.

Resolved: The council unanimously agreed that service providers must do the following to uphold this right:

• Document what security standards they follow, which security standards they adhere to and what processes they use.
• Furnish an audit statement of their data security practices.
• Share these documents with consumers to the extent that good security practices allow.
• Notify consumers within a specified time frame of any potential security breaches.
• Describe the incident notification process in contracts, and specify indemnifications if they do not live up to these terms.
• Provide audit statements that their business continuity plans work.
• Guarantee that the same security standards apply in the backup environment of the business continuity plan as apply in the primary environment.

7. The responsibility to understand and to adhere to software license requirements

The Problem: Software licenses for on-premises deployments can be confusing enough, and cloud deployments simply add to the number of questions. For example, can the consumer transfer licenses from an on-premises deployment to a cloud deployment? In general, software vendors do a poor job of explaining the possibilities and requirements of software licenses for cloud computing. The responsibilities lie more with the service consumer in partnership with a vendor than with the cloud service provider. However, service providers may place themselves at risk should they fail to recognize or limit their liability with regard to non-cloud-oriented software licenses being used inappropriately for cloud deployments.

The Council's View: Service consumers need to understand the license rights required for cloud computing, or they may incur unexpected costs or lag time to move software onto the provider's platform. But not all software vendors offer this clarity. In part, the lack of clarity stems from the lack of uniformity in licensing across the software industry. Different software vendors have different licensing models and terms, which they apply in different ways. For example, one vendor's enterprise license may work on either the customer's own rack space or in the cloud, while another vendor may require a different license or an additional fee to move software into the cloud. Thus, service providers cannot generically define license rights for all consumers.

In addition, the provider cannot grant all license rights that the service consumer needs. The consumer must obtain licenses and learn what rights they include when it buys software from a vendor.

Cloud computing also introduces new wrinkles into software licensing that providers and consumers have not yet worked out:

• Can a license to run software on a physical server also work to run it on a virtual server?
• Can and should licenses be transferred to a provider since the software runs on an architecture that the service consumer does not own?
• Could software running on a provider's architecture be transferred somewhere else—say, to another provider if the consumer switches?
• Does a service provider need its own license to run the service consumer's software or is the consumer's license enough?
• If a provider merged or went out of business, would the license rights it holds transfer to the new owner?
• If a service consumer gives 50 licenses to a provider but only uses some of those licenses now, can the provider give the unused licenses to other service consumers?
• How will a provider guarantee that it is upholding the terms of a software license, particularly if the service consumer supplies the software?
Providers and consumers must come to an understanding about how the proper use of software licenses will be assured. On the one hand, providers must be held harmless if the service consumer puts the software it licenses from a third party in the cloud yet violates the licensing agreement. On the other hand, the provider should not agree to an audit directly by the vendor if the consumer owns the software licenses. The service consumer must take charge of the audit because it needs to consider the whole context—both what the consumer runs in the cloud (perhaps using several service providers) and what it runs on its own infrastructure.

Resolved: The council viewed this issue as the one responsibility of service consumers it wished to introduce at this time. The council unanimously agreed that the parties involved in cloud computing must do the following to uphold this responsibility:

- Service consumers must establish that license agreements are not violated when moving software to the cloud.
- Service consumers and software vendors must agree to contracts that hold the service provider harmless if the consumer violates its licensing agreements by putting software in the cloud.
- Software vendors must provide license usage terms that do not create dual payments for the same capabilities offered under the original software licenses. A terms-of-use statement must cover both types of deployment.
- Providers must provide a clear statement in their terms of use that licensing rights must be established by the service consumer and software vendors and are not the responsibility of the service provider.
- Providers should state whether service consumers can acquire software or software bundles through the provider, which may source it from an independent software vendor or partner.

Conclusion

These seven rights and responsibilities will benefit both service providers and service consumers. Respecting them will require effort and expense from providers, but securing them will encourage enterprises to put more of their business into the cloud. These rights and responsibilities will enable service consumers to make more informed decisions before signing up with a provider—they can use them today as a checklist of questions to ask providers. But these seven rights and responsibilities will not become a reality unless enterprises insist upon them when they negotiate with service providers. And enterprises must also take on the additional responsibilities the rights imply. We urge all enterprises to do what they can to establish these rights and responsibilities as the standard for cloud services.
DEAN DEL VECCHIO
CIO and Chief Administrative Officer
Dow Jones
Dean Del Vecchio is responsible for shared global infrastructure and application services, information security, business continuity planning, enterprise architecture, project management, strategic sourcing and IT governance. He provides day-to-day management as well as strategic planning of all operational and administrative services globally, comprising accounting, general services and global real estate.

JOSEPH FLYNN
CIO
Lincoln Laboratory, Massachusetts Institute of Technology (MIT)
Joseph Flynn’s expertise is large-scale business transformation projects in which technology is the underlying enabler. He brings disciplined project management, expert business and financial analysis, organization design, business process design and change management skills to his projects.

MICHAEL GABRIEL
Executive Vice President, Information Technology and CIO
Home Box Office (HBO)
Michael Gabriel is responsible for overseeing HBO’s systems development and information management, computer center, communications and office systems. He has held the position of CIO since June 1999.

JAMES KLINCK
Vice President IT Security and Compliance
American Life Insurance Company (Alico)
Jim Klinck has responsibility for the development and management of Alico’s IT security and compliance program worldwide. The company is one of the largest and most diversified international insurance companies in the world, with operations in more than 50 countries.

JØRN LARSSEN
Senior VP Corporate IT
The Orkla Group
The Orkla Group consists of many local and global companies of different sizes and has fairly high dynamics due to mergers. Approximately 50% of Orkla’s employees are connected to the IT infrastructure.

EARL NEWSOME
VP Global IT Services
Estee Lauder
Earl Newsome leads Estee Lauder’s technology group in meeting challenges arising from the business’s need for reliable and responsive technology infrastructure and operations. The group is the platform and the foundation upon which global information services products and services are delivered.

SHREEKANT MOKASHI
Chief of Group Information Services
Tata Steel
Shreekant Mokashi is responsible for delivery of all services, projects, infrastructure, security and applications across the Tata Steel group. He drives usage of IT in business process improvements.

BILL PIATT
CIO
International Finance Corporation (IFC)
At IFC, Bill Piatt implemented a new operating model, sourcing strategy and organizational structure that resulted in a more than 50% increase in project delivery. He is now actively engaged with the newly appointed World Bank Group CIO to establish a federated IT delivery structure across the group.

DARIO SCAGLIOTTI
CIO
Pirelli
Dario Scagliotti coordinates and implements IT, as well as business process innovation strategies worldwide. He has direct IT responsibility for all the company’s business units.

THOM SNEED
CIO
Marathon Oil
Thom Sneed is responsible for information technology strategy and delivery for Marathon globally. His responsibilities span all business segments including corporate, exploration, production, refining and marketing. He also chairs the American Petroleum Institute’s Information Management and Technology Committee.

KEN THEIS
CIO
State of Michigan
As the CIO for the State of Michigan and director for the Michigan Department of Technology, Management & Budget, Ken Theis heads an agency of nearly 2,500 employees providing quality, cost-effective business services through a fully integrated information, communications and technology-infused service organization. He has extensive background in transforming business processes and developing successful teams to tackle the most complex projects.

SERGIO VEZZA
IT Director, Latin America
Anheuser-Busch InBev
Sergio Vezza has held various positions with Anheuser-Busch InBev, including in sales. Besides ensuring competitive cost and reliability in the region, seeking technological innovations for business and cloud computing is one of the company’s major 2010 initiatives.
DAVID MCCOY  
Managing Vice President and Gartner Fellow Emeritus  
Gartner  
David McCoy has co-led the Gartner Fellows program, managed the application integration research team, initiated or co-initiated Gartner business process management and business activity monitoring research, and led the team building Gartner research operating and governance models. He is currently team manager of the business process management group and researches business process management, business rule management and cost optimization.

DARYL PLUMMER  
Managing Vice President and Gartner Fellow  
Gartner  
Daryl Plummer is chief of research for emerging trends and manages the Gartner Fellows program, which is designed to allow senior analysts the opportunity to explore new research ideas. He is a primary analyst in cloud computing, service-oriented architecture, business process management and emerging trends.

To learn more about the councils and link to other council documents as well as related research, visit gartner.com/globalitcouncil or contact your Gartner account executive.

We welcome your comments or feedback. Please e-mail us at: globalitcouncil@gartner.com.