



DIGITAL TRUST IN THE CLOUD

LIQUID SECURITY IN CLOUDY PLACES



CSC

CSC.COM

BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING

EXPLORING SECURITY AND
TRUST IN THE CLOUD

THE PAYOFF POTENTIAL OF
DIGITAL TRUST IN CLOUD
PROCESSING

RONALD B. KNODE, AUGUST 2009



Digital Trust in the Cloud

Liquid Security in Cloudy Places

Table of Contents

When It Rains, It Pours	3
What Happens in Clouds?	4
Clouds Are Cloudy	5
The “Cloud Effect” on Digital Trust.....	5
Moving Out of the Data Center Further “Darkens” the Cloud.....	6
Not All Clouds Look Alike.....	8
The Real Value Question for Cloud Processing.....	10
Clouds in a Government Climate	11
Mandatory Doctrine.....	11
Is the government IT climate different in different places?.....	12
Can a cloud exist in the big picture of the government IT climate?.....	13
Classified Data	14
Elements of National Policy Projection ... Including Combat.....	14
What if ... clouds in a cyberwar?.....	14
Can international agreements brighten the sky for cloud processing?	14
The cloud effect in national policy	15
Government Clouds Are Already Overhead!.....	16
Dancing in the Cloud Today.....	18
Early Into the Cloud	18
Weatherproofing the Cloud to Provide Some Digital Trust	21
CSC Trusted Cloud Services: Liquid Security to Brighten the Cloud.....	24
CSC Trusted CloudVision	25
CloudTrust Protocol (CTP).....	27
Elements of Transparency	28
CSC Trusted Cloud Services at Work.....	30
The Last Word	32



Digital Trust in the Cloud

Liquid Security in Cloudy Places

When It Rains, It Pours

“When it rains, it pours.” First seen on the side of a Morton’s salt container in 1914,¹ the slogan traditionally referred to the easy flow of salt, even when clouds (and humidity) are present. In that case, the payoff was the ready dispensing of the salt itself *whenever it was needed*.

Today, however, information technology (IT) conversations about clouds refer to an altogether different payoff. In particular, the enterprise IT payoff is sought in the ready “dispensing” of IT infrastructure, platforms, storage, software, and even business processes *whenever they are needed!* And, such dispensing occurs not “in spite of” the cloud, but *right from the cloud!*

As exciting as these conversations are, they all begin with an attempt to define just what “cloud processing” (or “cloud computing”) really means. There is no conventionally accepted definition of cloud computing today, despite the many attempts to form a consensus. Definitions spill from universities, industry analysts, vendors, integrators, governments, trade publications, and service providers of all kinds.² None are yet widely accepted as an authoritative standard, and there is even tongue-in-cheek speculation that the many definitions “almost outnumber the many vendors vying for the potentially lucrative market share that exists.”³

However, despite the ambiguity shrouding the phrase itself, the implied payoff is just too exciting to ignore. Taken to its rhetorical conclusion, cloud processing promises to pour utility-like IT capability onto the processing needs of an enterprise just as it is needed, only as much as is needed, and only for as long as it is needed. Following the model of other “utility” services where we seldom trace origins, intermediaries, or delivery paths (compare with electricity, natural gas, and water), cloud processing brings the wonderful property of “elasticity.” Think of it! IT deployments and costs rising and falling with business and mission needs, scaling up when successful and down (and out) without regret costs when not so successful. It is this hazy promise of “elastic IT”⁴ lurking within the fuzzy boundaries of cloud processing that so attracts attention and investment.

But wait! Conventional cloud processing also promises to pour new showers of security and compliance problems. The abstraction and separation of applications and services from the underlying platforms and infrastructure that supports them, usually supported by virtualization, invalidates many security foundations used to support controls, and introduces entirely new threat surfaces that jeopardize historical control assumptions. For many enterprises, such circumstances dictate keeping anything and everything in-house, elasticity or not.

Can we capture the elastic payoff by putting trust in the cloud? Can we “trust in the cloud?”



What Happens in Clouds?

If the potential payoff is so tantalizingly large, then what exactly is happening in cloud processing that is preventing the capture of those payoffs at an enterprise level? After all, we have been using IT outsourcing and even grid computing at the enterprise level for some time now, and have been capturing the benefits of those styles of shared and distributed system operation and management. What makes cloud processing so different? Why is there such hesitation in enterprise attempts to capture it?

Attempts to answer to those questions are as legion as the definitions of cloud processing itself. For example:

- The University of California at Berkeley identifies a “top 10” list of obstacles for cloud computing ranging from service availability, data lock-in and data confidentiality to scaling, reputation fate sharing, and software licensing.⁵
- Ray Ozzie of Microsoft adds “latency” and a few other worries to CIO-level concerns about security, governance, and data integration.⁶
- Nicholas Carr, author of *The Big Switch: Rewiring the World, from Edison to Google* (W.W. Norton, 2008) predicts acceptable reliability, emphasizes the discerning use of the cloud to eliminate serious confidentiality issues, and lists “vendor lock-in” as a leading source of concern.⁷
- A special survey of business technology professionals by InformationWeek Analytics showed that “security” outpolled all other concerns (performance, control, vendor lock-in, support, configurability, speed to activate) by at least 20 percentage points.⁸

Whatever sample of cloud processing problems and risks are used, the sources of enterprise reluctance to engage in cloud usage can be parsed into three main “lacks”:

1. *Lack of standards.* All clouds are different. Each one must be investigated and analyzed to understand its capabilities and weaknesses. The technical basis for digital trust⁹ must be created for each cloud.
2. *Lack of portability.* Every cloud creates its own processing climate. Any digital trust obtained by one cloud environment does not transfer to any other.
3. *Lack of transparency.* All clouds are opaque. Neither technology nor process is easily visible. It is almost impossible to generate digital trust when transparency is absent.

And, while all three have some security contribution, it is the third “lack” – i.e., the lack of transparency – that contributes most to the enterprise anxiety about cloud security. This lack of transparency makes digital trust hard to create, and enterprise-class payoffs hard to collect.



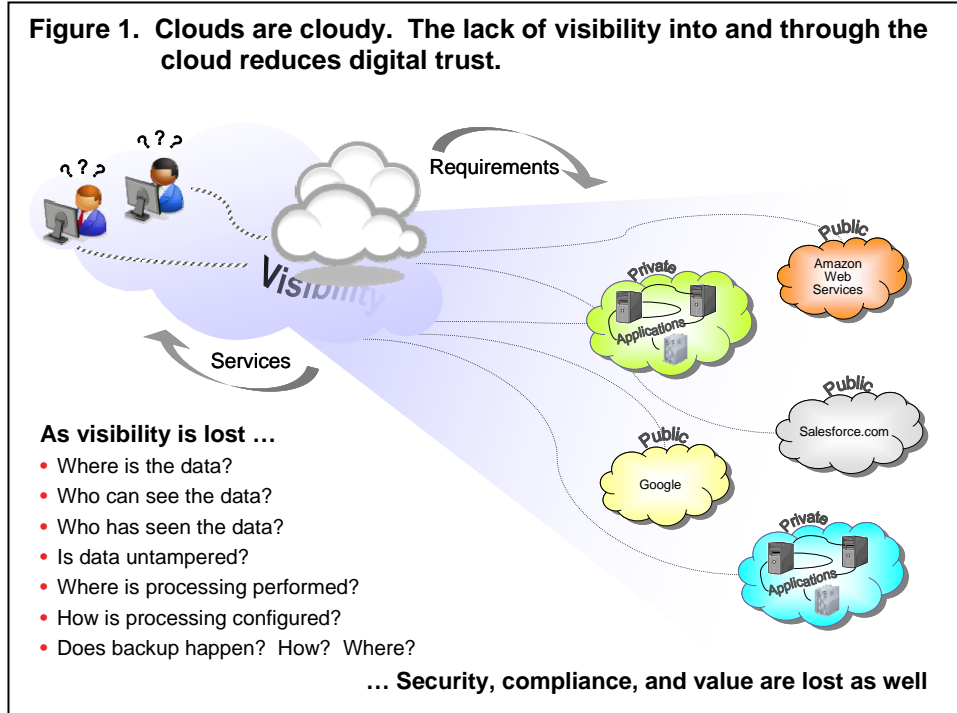
Clouds Are Cloudy

The “Cloud Effect” on Digital Trust

It is the very nature of clouds to be “cloudy.” The murkiness of nature’s clouds hides the sun, moon, stars, buildings, planes and even other clouds. That same effect occurs in cloud processing. But, instead of nature’s objects being hidden, it is data and processing objects and connections and other IT activities that are shrouded. As

illustrated in Figure 1, this “cloud effect” naturally masks the very information needed to generate the *evidence-based confidence* that leads to digital trust. Cloud processing obscures visibility to processing facts that are needed to confirm that whatever happened was supposed to happen ... *and nothing more*; that controls are doing what is claimed ... *and nothing more*. This kind of information forms the evidence that creates confidence in the technology and its operation. This evidence becomes the foundation for digital trust in the cloud. (See the sidebar “A Trusted Cloud.”)

Without information about such things as data and processing status, (all) processing and storage configurations being used, the location and topology of processes and data, the permissions and history of access and usage, backup timing and location(s), and user authorizations, there is no basis for any IT control verification.¹⁰ Consequently, the loss of



A Trusted Cloud

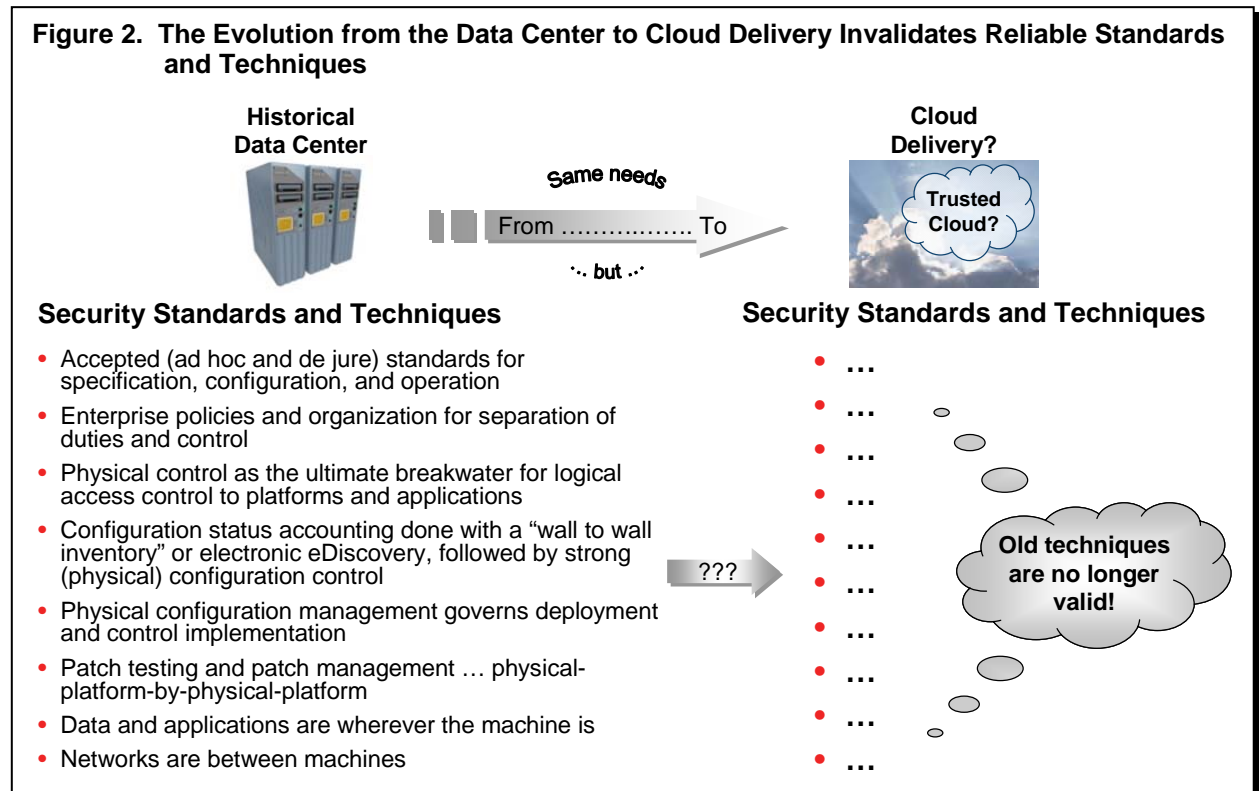
The consequences of the cloud are even more serious than just the loss of control. Whenever evidence-based confidence is lost, then there is a digital trust deficit. When there is a digital trust deficit, then new enterprise value cannot be created (and some current enterprise value can even be put at risk). These realities are as true for cloud processing as any other style of IT. What we desire is nothing less than a trusted cloud – i.e., a *cloud that harmonizes the security for transactions and data with comprehensive transparency of control and result, such that it conveys evidence-based confidence that systems within its environment operate as advertised, and that no unadvertised functions are occurring.*



visibility into and through the technology and procedures used in cloud processing makes full “on-demand” accountability and end-to-end audit impossible. When visibility is lost, security, compliance, and, ultimately, enterprise value potential are lost as well. In other words, without visibility into and through cloud processing, there is inevitably a digital trust deficit in the cloud.¹¹

Moving Out of the Data Center Further “Darkens” the Cloud

As if the fog of cloud processing itself is not enough, the transfer of processing out of the data center and into the cloud further darkens the mist, and makes even more difficult the generation of trust in the cloud. Figure 2 samples the effects of this transfer, showing how cloud



processing invalidates traditional techniques for security control verification, leaving the enterprise with no independent alternative for security validation and (ultimately) digital trust generation. A lot of the tools and techniques we have depended on for security, control and compliance all of a sudden “disappear” in the cloud, and we are left to grapple with fundamental questions of control without any reliable audit capacity.

Moreover, many of the control foundations sampled in Figure 2 become invalid when the cloud is implemented with an *abstraction* methodology. The abstraction methodology most frequently mentioned and applied is *virtualization*,¹² although this is not always the case (Google being a primary example¹³). Still, virtualization has become indelibly connected as a primary technology used to deliver the “elasticity” of cloud processing. In fact, some industry participants go to the limit in equating virtual processing technology and cloud processing. For instance:

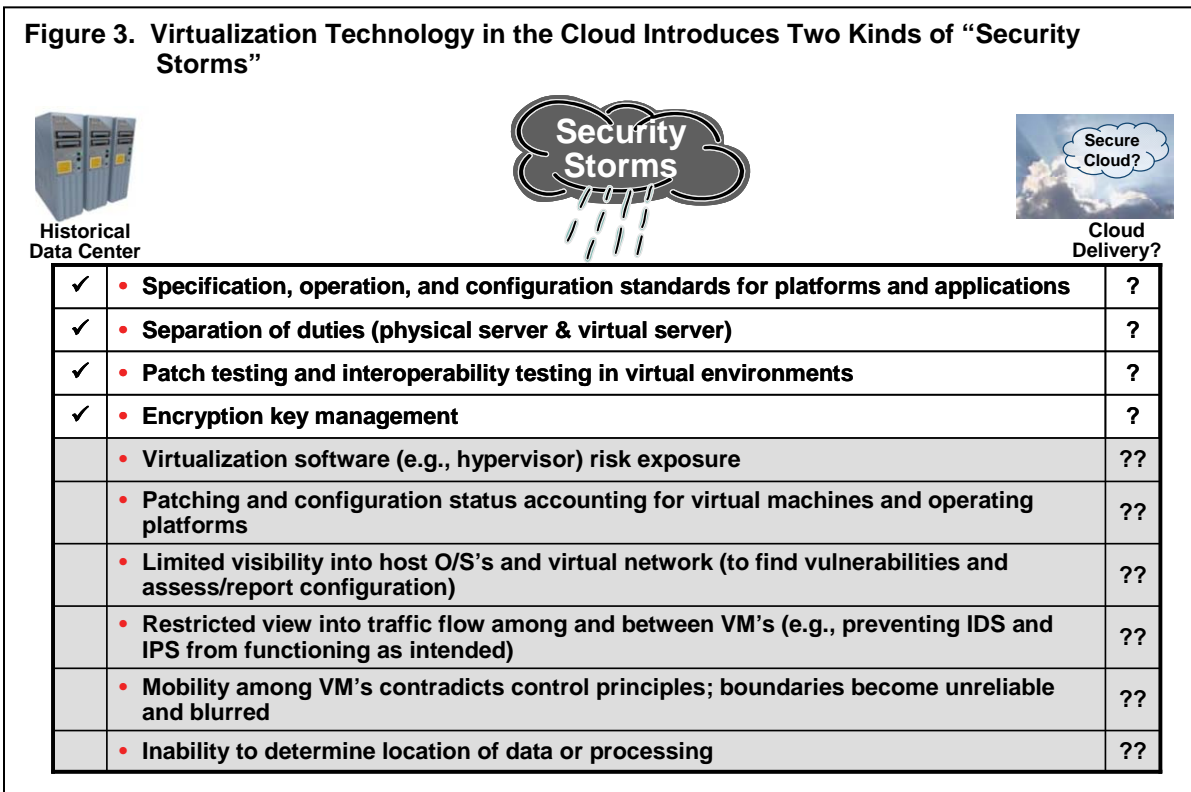


- “Without virtualization there is no cloud.” Shaun Walsh, vice president of corporate marketing at Emulex.¹⁴
- “I don’t think that cloud computing would be possible without virtualization.” Peter Nickolov, president and CTO at 3tera.¹⁵

Therefore, although server virtualization is not equal to cloud processing, creating digital trust within virtual configurations (or otherwise abstracted configurations) becomes an important step in creating digital trust in the cloud.

However, the introduction of virtualization technology (or other abstraction techniques) not only invalidates traditional security techniques as suggested in Figure 2, but also introduces new threat surfaces that generate new potential for digital trust deficits and real digital trust penalties. For instance, the sample table shown in Figure 3 presents examples of two kinds of “security storms” that we find in cloud processing:

1. Security storms that emerge when *existing standards or techniques* that can deliver evidence of security control in traditional data center settings are suddenly invalidated due to the use of virtualization technology and virtualization management (or other abstraction techniques). See the unshaded rows in Figure 3.
2. Security storms that represent *entirely new threats and requirements* for security evidence, for which there is no historical analog in traditional data center operation. See the shaded rows in Figure 3.





Techniques for digital trust creation are especially perplexing when we consider the brand new threats and requirements of the second (shaded) category. What do we measure or monitor or respond to when the circumstance is brand new? For instance, how is network intrusion detection manifested in a virtual configuration when the network no longer exists solely on traditional wired or wireless mechanisms, but now (virtually) exists in and between abstracted platforms? Or, how are national (citizenship) processing restrictions enforced with virtual (abstracted) platforms that can automatically migrate from place to place frequently and quickly? Or, how do we sustain confidence in processing configurations that match our “security standards” but are only virtually resident on otherwise abstracted platforms, which themselves could be in risky configurations?

Clearly, the new threat surfaces present new potential for digital trust deficits. But, when digital trust is created to deal with this new era of abstraction in cloud processing, the enterprise payoffs can be enormous.

Not All Clouds Look Alike

The cloudiness of clouds is pervasive. Despite the ambiguities of definition, all clouds come with some degree of the “three lacks.” However, as in nature, not all cloud processing systems look alike. In the pursuit of clarity and control, organizations have applied different styles of cloud deployment, and these different styles can reduce (or increase) the amount of cloudiness that must be handled. In other words, the style of cloud deployment used can actually create some digital trust in the cloud by reducing the impact of one or more of the “three lacks.”

The U.S. National Institute of Standards and Technology (NIST) refers to these styles of deployment as deployment models and has offered the definitions shown in Figure 4. Since a cloud deployment model is itself a technique for reducing a digital trust deficit, and since the deployment model is one of the techniques most used today by enterprises that need to generate additional digital trust in clouds, these deployment models have become central to the exploration and early use of cloud processing.

Figure 4. Cloud Processing Deployment Models from NIST Working Definition¹⁶

Deployment Model	Description
Private Cloud	The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
Community Cloud	The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
Public Cloud	The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.

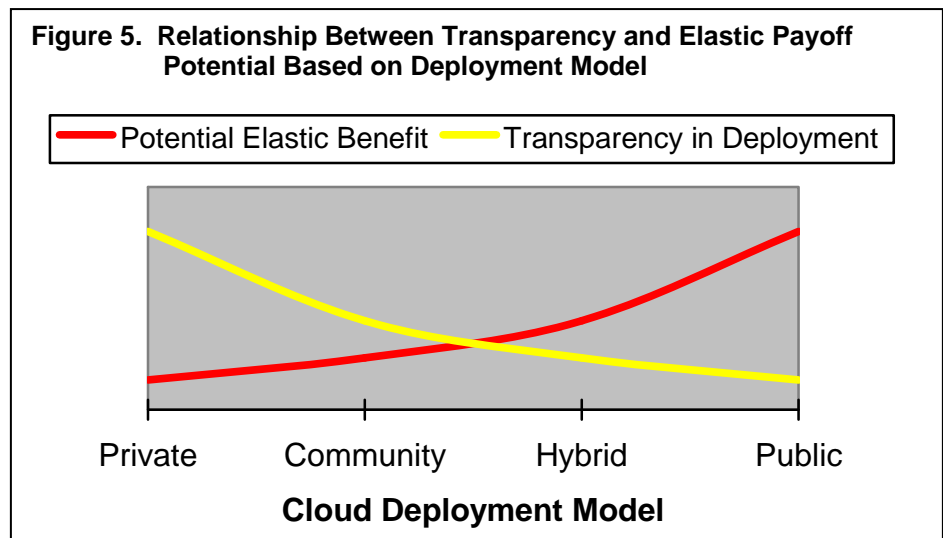


Figure 4. Cloud Processing Deployment Models from NIST Working Definition¹⁶

Deployment Model	Description
Hybrid Cloud	The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting).

Although the deployment model technique can be used to create digital trust (by reducing the cloudiness of cloud systems), this technique can also have the detrimental side effect of reducing the elastic payoff potential normally sought in cloud processing. For instance, private clouds (by definition) exist solely for a single organization and so can be specified and operated according to the policies, standards and requirements of that organization. Under these circumstances, a private cloud becomes a flexible extension to traditional data center operations and thereby suffers few transparency issues. But, also under these circumstances, the elastic payoff potential depends exclusively on the workload and functional needs of that single organization. Therefore, the elasticity is greatly reduced, the payoffs become smaller, and the (private) cloud itself is less utilitarian.

On the other hand, public clouds increase the elastic payoff potential, but do so by reducing transparency. Consequently, digital trust must be created in other ways. This relationship between transparency and the elastic payoff potential based on deployment model alone is illustrated in Figure 5.





The Real Value Question for Cloud Processing

In light of the inverse relationship between transparency and potential value capture (elasticity), the central question for enterprises anxious to use (more) cloud processing now becomes how to reverse that relationship:

“How do we create digital trust in the cloud so we can reap the greatest elastic benefit?”

And, since the creation of digital trust is tied closely to the introduction of greater transparency into cloud processing, then this question can be rephrased as:

“How do we bring transparency to the cloud so we can reap the greatest elastic benefit?”



Clouds in a Government Climate

All industry sectors, including government, seek benefit by including cloud processing in their IT programs. Each sector, no doubt, has unique interests and concerns. But government has a special obligation beyond responsible due diligence on behalf of a traditional community of enterprise stakeholders, i.e., customers, employees, and owners. Government IT planning must satisfy not only specific agency, ministry or departmental interests (traditional stakeholders) but also the larger obligations for “national health and safety,” even as cloud processing potential appears to increase. This extended obligation brings with it different circumstances and needs for cloud processing in government. The government “operating climate” is, in fact, different from typical commercial operating climates, and this difference in operating climates affects both the speed and extent of cloud processing payoff potential that government can capture.

The government operating climate differs from other enterprise climates on at least three fronts:

1. *Government-wide doctrine is mandatory.* The application of security and information processing standards is not a matter of choice for each agency – i.e., not an item to be traded off as part of a risk/reward equation.
2. *Government data can be nationally classified, and therefore it is directly subject to laws and consequential impacts* of non-compliance by both data owners and system operators.
3. *Government preservation and projection of national health and safety using IT has become an element of national policy*, including combat. Jeopardizing national health and safety with inappropriate use of different kinds of IT can have enormous national consequences.

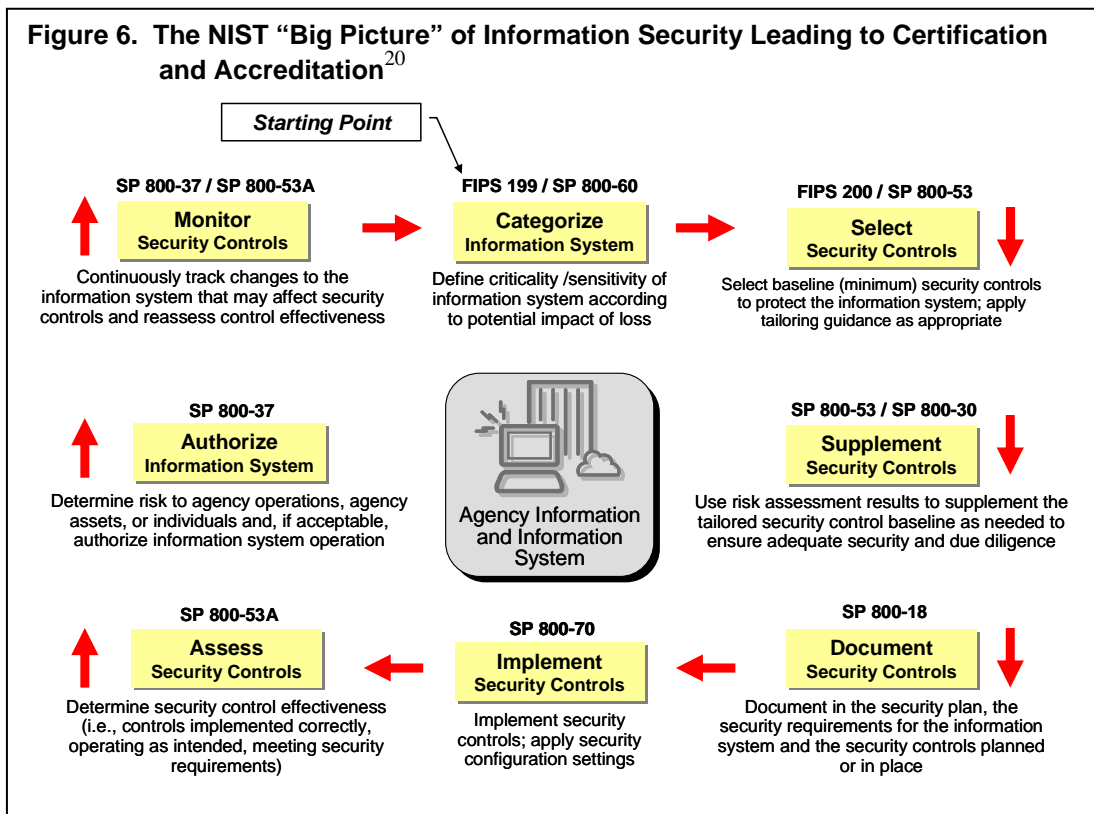
These three fronts dictate in great measure just how the government must seek digital trust in the cloud before making cloud processing a part of its IT strategy. Each front reinforces the need for transparency into and through the cloud. While the barriers to cloud processing due to the lack of standards and portability apply to government as well as industry, it is the lack of transparency that represents the biggest obstacle to widespread application of cloud processing (in all of its manifestations) within government. (Recall the three “lacks” on p. 4.)

Mandatory Doctrine

With each passing day, security is becoming more and more a standard part of the government acquisition and operational lifecycle. Whether designed and developed “in house” or prepared by a contractor, government system development, deployment, and operation incorporate an ever-expanding consideration for security, including some non-negotiable steps for establishing the “trustworthiness” of systems. This evolving lifecycle that continues to incorporate security issues and responses as a must-have part of the process is the genesis of a government IT climate that is relentless in its pursuit of verifiable control structures.



For example, in the U.S., the Office of Management and Budget (OMB) Circular A-130 requires a security *accreditation* (a management decision), which itself involves a security *certification* (evaluation against a technical standard).¹⁷ Furthermore, that same Circular directs all agencies and departments of the U.S. federal government to comply with the Federal Information Security Management Act (FISMA¹⁸) as well as the Computer Security Act of 1987. In so doing, OMB has further announced that the U.S. National Institute of Standards and Technology (NIST) Special Publication 800 series of documents is now required (by FISMA),¹⁹ leading to an unequivocal set of actions to make sure security needs are identified and covered. Moreover, this entire certification and accreditation (C&A) process, as instructed by NIST, includes a set of system security planning, categorization, assessment, analysis, examination, testing, and documentation activities to deliver the evidence that can substantiate agency and developer



claims of security. That “big picture” around information system security (aimed at a sustained C&A) for the U.S. federal government is reflected in Figure 6.²⁰

Is the government IT climate different in different places?

Does this risk management situation change under special circumstances? Are there any places in government where the constraints of the “big picture” of Figure 4 do not apply? For example, some would look to agencies and departments outside the specific jurisdiction of NIST guidelines and standards. Others might look to doctrine outside the U.S.

All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.



- *What about U.S. Defense and Intelligence Agencies?*

In addition to OMB Circulars and numerous federal laws (e.g., Federal Information Security Management Act of 2002 (FISMA), Computer Security Act of 1987, Health Information Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act, and even the American Reinvestment and Recovery Act of 2009), there are also U.S. departmental policies and special content extensions to this general requirement for a thorough and structured process for developing and substantiating security properties of federal systems. For instance, the U.S. Department of Defense (and other agencies) now applies the Defense Information Assurance Certification and Accreditation Process (DIACAP),²¹ which follows the same general methodology as is outlined in Figure 4. The DoD instruction does, however, invoke its own set of controls and control relationships according to DODI 8500.2²² rather than NIST Special Publication 53. Such is the case as well for the other variants of C&A process currently found in the U.S. government.²³ Terminology, focus and granularity are different, but the resulting consequence is not.

- *What about other countries and governments?*

The U. S. government is not alone in its devotion to an information risk management framework that balances risk, threat, sensitivity, control, and accountability. In just about every developed nation we find analogs to the doctrine promoting a mandate for official “certification and accreditation” to establish a control baseline and ongoing accountability.²⁴ So, government clouds are cloudy everywhere ... not just in the U.S.

Can a cloud exist in the big picture of the government IT climate?

An examination of this “big picture” outline of the information security obligation of U.S. government agencies and departments highlights the importance of full visibility into the information systems being designed and deployed. But, the basis of system control according to NIST Special Publication 800-53 is a combination of technical, management, and operational safeguards based on the assessed level of value provided by a system and the assessed level of threat/risk the intended system is expected to face.²⁵ Without transparency, how can IT technical controls (e.g., auditing, access control, system configuration, encryption) be selected, documented, supplemented and tested/assessed? Without transparency, how can management controls (e.g., vulnerability assessments, risk assessments, system and service acquisition) be established and confirmed? And, without transparency, how can operational controls (e.g., configuration management, awareness and training, change management), be observed, evaluated and affirmed? When transparency is lost, the ability to generate “evidence-backed confidence” is lost as well. Consequently, the ability of government IT climates to use cloud processing today is limited by current doctrine and mandatory practice.

Doctrine and standards and policy will each have to evolve further to include cloud processing more completely in government IT climates (including all types of cloud delivery models). That is precisely one of the objectives of current government trials and experiments with cloud processing. (See “Government Clouds Are Already Overhead!” on p. 16 for some examples of those early government applications and experiments.)



Classified Data

Only governments can nationally classify data. And, with force of law, violation of rules in the handling of classified data can have very real personal consequences, including loss of job, fines, and imprisonment. While we see similar kinds of legal consequences for mishandling data that is other than classified – e.g., privacy data under HIPAA²⁶ and financial disclosure under Sarbanes-Oxley²⁷ – the rules for identifying and handling nationally classified data are unequivocal, and the penalties can be quite severe.²⁸

Cloud or no cloud, transparency is essential for handling classified data. For example:

- Without transparency, there can be no confirmed chain of custody for information.
- Without transparency, there is no way to conduct investigative forensics should an unauthorized disclosure be suspected.
- Without transparency, there would be little confidence in the ability to detect any attempts or occurrences of illegal disclosure.

When considering classified data, the conditions for cloud processing are clear. Digital trust in any kind of cloud processing intended for classified data must come with deep transparency into the technology, the processes, and the people involved. Otherwise, it cannot be applied.

Elements of National Policy Projection ... Including Combat

Information technology has become an element of national policy projection, including a technique for combat. The cyber war examples of Estonia in 2007²⁹ and Georgia in 2008³⁰ provide testimony to the combat support use and effectiveness of IT across an anonymous and ubiquitous Internet. Though unconfirmed, suspected North Korean attacks on U.S. and South Korean Web sites have also been reported as recently as July 2009.³¹

What if ... clouds in a cyberwar?

Each of these examples was rewarded with different levels of success, ranging from a near economic and government shutdown (Estonia) to an annoying (but preventable) waste of processing cycles on public Web sites (North Korean attacks). However, imagine what might have happened if everyone in Estonia were receiving their email service from a single cloud provider, or every military echelon in Georgia were processing their periodic strategic plan updates in an infrastructure-as-a-service cloud with computing and storage services! The consequences could very well have been much more severe.

On the other hand, imagine what *could* happen if techniques for bot infection of cloud processing environments succeeded! What combat support effect could such a controlled cyberattack element have when transparency is lacking?

Can international agreements brighten the sky for cloud processing?

Each of us can imagine other scenarios that would highlight the dangers of cloud processing, or highlight the cyber-advantage that a technique could provide, or both. Governments around the world have already acknowledged the growing threat of cyberwar (with or without cloud

All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.



processing), but little progress is being made in achieving international protocols and conventions to account for such actions. The U.S. and Russia, for example, remain locked in a fundamental dispute over how to counter this threat, even though both nations agree that cyberspace is an emerging battleground.³² Without transparency, cloud processing amplifies the risks that international disputes over cyberwar will become more frequent or more heated, if only because cloud usage could concentrate the impact of cyberwar techniques, both offensive and defensive.

Today no one can predict the likelihood of international agreements providing some structure and control around IT usage as a public policy projection. But, such an agreement is likely to include some verification provisions. In that case, digital trust in the cloud is essential to pursue a “trust but verify” policy as applied to cloud processing.

The cloud effect in national policy

Even as they take their first trial steps into cloud processing, governments around the world are not waiting on international agreements to satisfy their need for digital trust in the cloud (or IT in general). In the U.S. the Defense Industrial Base (DIB) program of the Department of Defense establishes a partnership between the U.S. DoD and its suppliers. That partnership establishes new control requirements and reporting requirements on private infrastructure used in support of defense needs (for Controlled but Unclassified Information – CUI) in return for better threat data. Those requirements apply to cloud processing just like any other processing. In addition, the U.S. Comprehensive National Cybersecurity Initiative (CNCI)³³ adds even more cyber-elements to the national cyber policy capability of the U.S.

But, it's not just the U.S. that is pursuing a greater role for cyber-capacity as an element of national policy. For example, the Canadian Department of National Defence (DND) is establishing a mutual awareness and assessment program to match the U.S. DIB.³⁴ Australia has its own Defence Industry Security Program (DISP) of similar capacity and intent.³⁵ And, the U.K. has published its latest plans in the “Digital Britain” final report³⁶ and in the “National Security Strategy of the United Kingdom.”³⁷ This sample can be extended to many other governments as well.

All of these national policy statements for IT use apply to cloud processing as well as every other kind of IT application being used by these governments. The cloud effect is becoming a part of these national policies. The greater the use of cloud processing, the greater the need for digital trust in the cloud to be fully in line with these public policies (through transparency, standardization and portability), and for enabling enterprises of all kinds to capture the payoffs of cloud processing.



Government Clouds Are Already Overhead!

All is not lost! Ironically, the unyielding transparency needs of government have not blunted attempts at experimentation and early application of controlled use of cloud processing. Governments continue to lead the way in research, trials, and experiments with cloud and “cloud-like” processing. In fact, despite the absence of digital trust in many types of cloud processing service delivery, governments are taking advantage of one particular model of cloud-service deployment where digital trust can be created “the old fashioned way.” In particular, *private clouds* are finding their way into new government uses nearly every day. So, even while new techniques for digital trust creation in cloud processing are being developed, governments today are still able to capture some of the elastic benefits of cloud processing by limiting their population, location, and use, and thereby reducing some of the opaqueness that exists in cloud processing.

In particular, we find an eager appetite for cloud processing in the U.S. government, even in advance of a standard definition and a list of required conditions for use.⁴² While the efforts span multiple agencies, they all share a common characteristic of solution. They are all examples targeting “private clouds,” representing one avenue of early attempts to seek digital trust in a cloud, even without a comprehensive solution to the “lack of transparency.”⁴³ Figure 7 lists four of the “private clouds” already built (or underway) and applied by the U.S. government.

Figure 7. A Sample of (Private) Clouds Developed in and for the U.S. Government

Owner	Name – Service(s)
Defense Information Systems Agency (DISA) ³⁸	Rapid Access Computing Environment (RACE) is a private cloud for DoD users that delivers infrastructure, platform, and software “as a service.” Although located entirely within the walls of DISA, RACE provides a public cloud-like experience with a Web portal, 24x7 availability, a service catalogue, and a credit card payment option. ³⁹
National Aeronautics and Space Administration (NASA) Ames Research Center ³⁸	“Nebula” is a combination of infrastructure, platform, and software “as a service” in a private cloud. Based on the Eucalyptus open source software, Nebula is initially targeted at the rapid development of secure Web applications, public outreach, collaboration, and mission support.
National Security Agency (NSA) ⁴⁰	A geographically distributed, collaborative intelligence gathering and “sharing” system in response to Intelligence Community Directive 501.
Department of Veterans Affairs (VA) ⁴¹	A small private cloud intended to provide an early warning system that could analyze data from over 100 VA clinics and hospitals and spot outbreaks of infectious diseases. Now named the Health Associated Infection and Influenza Surveillance System.

All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.



However, there are even more government (and industry) plans and activities targeting cloud processing payoffs well beyond the existing government agency and department cloud start-ups. For example:

- The U.S. General Services Administration (GSA) is releasing a Request for Proposals (RFP) for a “GSA Storefront” that lets government agencies shop around for cloud services from various providers.⁴⁴
- The Department of Energy National Laboratories are exploring the use of (private) cloud services for scientific computing, communication with the public, collaboration, and control over public cloud services.⁴⁵
- Major cloud providers (e.g., Google, Amazon, Microsoft, Salesforce) have all been attempting to qualify their cloud or cloud-like offerings under U.S. government criteria (e.g., FISMA) so that they could be ordered and used by government agencies in the same way they are used today by individuals and businesses.⁴⁶ For instance, Google has announced it is working to obtain FISMA certification and accreditation of its services by the end of 2009.⁴⁴ Amazon has set up an initiative called “Amazon Government Solutions” to target U.S. federal and state government clients, including the Department of Defense.⁴⁷ And Microsoft has introduced its own “Open Government Data Initiative,” a program aimed at helping government agencies host their data on Microsoft’s Windows Azure cloud computing platform.⁴⁸
- An online magazine, the “Government Cloud Computing Journal,” has been launched to offer stories and articles on the effective use of cloud computing technologies within the government domain.⁴⁹ Something must be up!
- The California Public Utilities Commission (PUC) began using “Open Campus,” an internal cloud of virtualized and unvirtualized x86 servers, to let employees log in to their applications from anywhere in the state.⁵⁰
- The U.K. government’s Chief Information Officer, John Suffolk, has been gathering input regarding the recommendation in the *Digital Britain* report for the U.K. government to create a “G Cloud,” a government cloud infrastructure for all public sector agencies and their applications.⁵¹

Governments are certainly exploring and experimenting with (mainly private) cloud services. The absence of digital trust for other styles of cloud delivery is just too much to tolerate for now. But, when transparency is returned and digital trust in the cloud is created, more and more government applications and services will become legitimate targets for the elastic payoff of cloud processing.



Dancing in the Cloud Today

Commercial enterprises as well as governments have recognized the potential payoffs that can be captured with cloud processing. Even though the cloud represents a new technology and service model, there are already significant enterprise examples and individual users who are “dancing in the cloud” – i.e., experimenting or sampling or even integrating cloud processing of some type (and by some definition) in their pursuit of business or mission objectives. Some users consider themselves as dabbling in the cloud, while others express an earnest and full commitment to cloud processing as an important part of their enterprise architecture and operation.

Early Into the Cloud

Early users of cloud processing come in all sizes (small, medium, and large enterprises), from just about every business sector, and in all stages of commitment and maturity of use. Conventional wisdom declares that small and medium sized businesses (SMBs) have been leading the demand for cloud processing services.⁵² After all, the individual cloud-delivered email accounts from just Google and Yahoo alone number in the tens of millions! That conventional wisdom is backed up by a business opportunity for cloud processing services in the SMB market that is estimated to be about \$30 billion!⁵³ The combination of a basic business need for fundamental IT services at reduced cost, along with the sheer number of SMBs, has produced a perfect storm of potential for cloud processing that continues to be a motivator for the implementation and application of cloud processing capabilities.

However, despite the acknowledged leadership of SMBs as the earliest adopters, cloud processing has found its way to enterprise scale applications. There is an ever-growing supply of preliminary case studies that span enterprise scale right up to the very largest organizations, representing different kinds of industries and interests. Just about everyone can find some example to illustrate a particular success or a specific caution even though the final chapters in these pioneering uses are still not written. Figure 8 provides a sample of commercial cloud uses. It mirrors the government examples shown in Figure 7. Together the figures illustrate the basic ways in which current organizations are trying to control their needs for digital trust in the cloud so that at least some cloud processing service can be used.

Figure 8. Sample of Commercial Cloud Uses

Enterprise	Cloud Processing Description
Educational Testing Service (ETS) ⁵⁴	ETS has created a program of aggressive exploration of public cloud services as a full part of its IT services plan. Beyond just pilot programs, ETS uses real applications (matching certain criteria) as the technique for examining and measuring the actual enterprise payoff potential from cloud processing. One of its earliest explorations involves a compute-intensive speech recognition application used for automated assessment of speech. Ultimately, the recognized speech is turned into a test result, and that collection of test results can be scored automatically. The ETS application

All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.



Figure 8. Sample of Commercial Cloud Uses

Enterprise	Cloud Processing Description
	<p>meets the important criteria of highly variable demand based on schedules and volume of tests given.</p> <p>But the ETS program has also investigated the circumstances and consequences of weak (or non-existent) service level agreements (SLAs), and the security issues stemming from a <i>lack of transparency and control</i> as services move into known public clouds. Two of the most important security circumstances for ETS involve intellectual property protection and the loss of data access control in the cloud.</p> <p>ETS responded to these concerns by applying its findings and conclusions about SLAs and public cloud security to its decisions about which applications are suitable for cloud service and which are not. Those findings generated additional constraints on acceptable applications, and those constraints are the means by which transparency issues are reduced and sufficient digital trust is created. Furthermore, ETS decided to maintain its own core processing capability for the application, and let the cloud service in Amazon’s Elastic Compute Cloud (EC2) be invoked as a “cloudbursting” response to surge needs. This is an example of how ETS has taken action to reconcile risk and policy compliance issues to find “safe” candidates for cloud processing.</p> <p>Now, ETS continues to hunt for practical applications that meet the safety criteria, and is moving forward with success using a very practical and very contemporary technique to establish enough digital trust to capture value wherever it makes sense.</p>
Towson University ⁵⁵	<p>Towson University made a practical decision in 2009 to proxy all the student email accounts to Google Gmail accounts. So, while students still have an email address of the form “name@towson.edu,” their real email is sent and received through Gmail. Faculty and staff at Towson University, however, continue to have their email supplied in-house.</p> <p>Once again, this split decision is pursued as a way to satisfy email needs without putting at risk the privacy policies and sensitive information managed by Towson faculty and administrators. In other words, digital trust is created by eliminating faculty from the transparency problem and letting students receive the payoff from the public cloud. In this case, students enjoy a far larger mailbox (measured in gigabytes) than do faculty members! That’s a pretty nice payoff.</p>
Bechtel ⁵⁶	<p>As the scope and geographic spread of Bechtel projects continued to enlarge, Geir Ramleth, senior vice president and CIO of Bechtel, found himself with challenges that even a recent IT modernization would not solve. For every 100 employees in the U.S. and Europe who retired, Bechtel had been able to replace only 60. More and more project locations needed support in 50 different countries around the globe. And, all of a sudden, about a third of the people accessing Bechtel’s network were non-Bechtel employees. Teams of employees, contractors, and supply chain partners in every part of the world were collaborating around the clock.</p>

All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.



Figure 8. Sample of Commercial Cloud Uses

Enterprise	Cloud Processing Description
	<p>Bechtel found itself in need of a new way to support these teams, including a full measure of “liquid security” to match the fluid support services.⁵⁷</p> <p>The just-completed modernization had streamlined IT systems and cut costs by nearly 30 percent, but these emerging support issues went beyond cost savings. Mr. Ramleth redefined the support problem with this question: “If we started Bechtel today, would we do IT in the same way we’re doing it now?” The answer, according to Ramleth, was “No.”</p> <p>So, after examining how post-Internet companies (that had a clean slate when they started) had designed and applied IT, he decided to follow the networking practices of YouTube, the standardized server approach of Google, the extreme virtualization of Amazon, and the multitenant application support strategy of Salesforce.com. As a result, Bechtel is growing its Project Services Network (PSN), the Bechtel private cloud that is designed to deliver secure, simple, ubiquitous, and rapidly deployable information service for all Bechtel teams everywhere. The PSN is Bechtel’s own SaaS offering for all of Bechtel’s project teams, delivering a “Google-like” experience through its PSN portal. Where more extensive versions of applications need to be supported, Bechtel will continue to support those in more traditional (fixed) fashion.</p> <p>Creating the Bechtel PSN as its own internal proprietary cloud solves a lot of transparency problems and generates enough digital trust for Bechtel to capture some value now, and explore just how such an undertaking can be used as an interim step to third-party (public cloud) SaaS offerings in the future.</p>
<p>General Electric (GE)</p>	<p>General Electric has adopted a “go slow” approach to cloud computing but has made big efforts and explorations into the possibilities for cloud processing. These efforts are organized into a three-year project to implement technologies that provide flexibility, automation, and manageability. Many of the efforts involve virtualization and virtualization management, ultimately extending into a capacity to manage virtual machines as a pool of resources rather than individually. This is the basis of GE’s exploration of its own private cloud capacity, including an examination of the various technologies that can support these objectives and the value they can deliver.⁵⁸</p> <p>But, GE’s exploration also extends to public clouds. For example, GE has been testing Google’s Gmail and productivity software for nearly two years,⁵⁹ and is moving to WebEx for Web conferencing. More recently, GE hedged its Google bets by adding Zoho online applications for Web-based spreadsheet editing and storage (while still retaining Microsoft’s Excel). In the words of GE’s CTO Greg Simpson, storing GE data on Google servers is “probably our biggest stumbling block to going bigger with Google.”⁵⁹</p> <p>In addition, GE has embraced software-as-a-service (SaaS) by purchasing Aravo’s Supplier Information Management (SIM) SaaS product. According to GE’s veteran CIO Gary Reiner, the fact that SIM was a hosted solution</p>



Figure 8. Sample of Commercial Cloud Uses

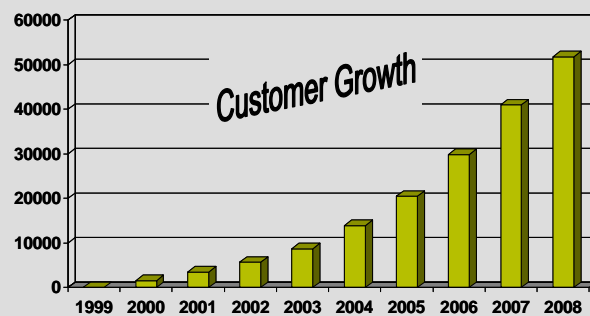
Enterprise	Cloud Processing Description
	<p>was immaterial to GE's decision.⁶⁰ GE needed a supply chain coordination system to support 100,000 users and 500,000 suppliers in six languages. Aravo's SIM is helping to satisfy that need.</p> <p>But GE is not immune to security worries about its data. GE claims to be confident that its supplier data is secure outside its own firewalls with Aravo. According to Reiner, that confidence is justified by one word: "Audits."⁶⁰ GE has chosen to reduce the transparency and digital trust deficits of cloud processing by using private clouds, and by applying the timeless technique of independent (and constant) inspection and auditing.</p>

The examples of Figure 8 are but a taste of the scope of enterprise use of current cloud processing capabilities, even without a ready capacity to create or discover digital trust in the cloud, and even without a standard definition of cloud processing! Today's scope is impressive, especially considering the relative newness of the service capability and the delivery model. (See Figure 9, "The Growth of Salesforce.com.") Such achievements would seem to indicate that cloud processing has "arrived" as a healthy contributor for enterprise IT.

But, the full story is not completely written based on samples from cloud service vendors. The growth achievement of Salesforce is indeed remarkable. And the progress made by the "early dancers" in the cloud is impressive. But, \$1 billion of cloud revenue compared to the total projected size of global IT spending for 2009 at \$3.2 trillion⁶¹ still leaves plenty of room for growth in cloud processing. And the limits on applications and deployment models to date still leave tremendous stores of untapped enterprise value. Much of that growth and value capture can only come when digital trust is delivered in and through the cloud.

Figure 9. The Growth of Salesforce.com

- Born in San Francisco in 1999
- Established force.com in 2008
- 1.5 million individual subscribers by 2008
- \$1 billion in cloud revenue by 2008



Source: Created from data at <http://www.techcrunch.com/2009/02/25/salesforce-hits-1-billion-dollars-in-annual-revenues/>

Weatherproofing the Cloud to Provide Some Digital Trust

Cloud processing is a fact of IT service today, even at enterprise scale. What started as a service technique that attracted individuals and SMBs has become a wave of possibility and potential for enterprises of all size, government and commercial. The "three lacks" – standards, portability, and transparency – still hinder the value potential for cloud processing (see "What Happens in Clouds?" on p. 4). Yet, today we are able to apply technologies and techniques to

All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.



reduce the transparency need, and generate enough digital trust to capture at least some value already. In fact, in just the few examples of Figure 7 and Figure 8 we see the three main contemporary techniques used to “weatherproof” the enterprise in its use of the cloud and obtain a value payoff. These techniques are used to compensate for the lack of transparency (and standards and portability) and generate digital trust in the cloud until these three “lacks” are removed by additional digital trust cloud technologies and practices. The three techniques are:

- *Private clouds.* This technique is a big eraser of transparency issues (as well as standards and portability issues). It is certainly the easiest technique to explain, though that ease brings with it the reduced payoff potential as illustrated in Figure 5. All of the widely-referenced government examples in Figure 7 depend on this technique to generate enough digital trust in the cloud so that cloud processing can be exploited to create value for the enterprise. The largest of the commercial examples in Figure 8 also exhibit this same dependency (GE and Bechtel).
- *Safe applications and data.* This digital trust creation technique is popular when a private cloud is *not* sought as an answer. In this case, enterprises constrain their choices of applications and data for the (non-private) cloud to those where the absence of transparency or SLAs can be tolerated. The mature ETS process described in Figure 8 is a splendid example of this technique. Using this approach, the amount of digital trust needed in the cloud is reduced by other compensating means. ETS, for example, retained a core capacity to deliver the (safe) application and used “cloudbursting” as necessary.
- *Presumptive security.* This is a *claims-based* technique and it can be misleading, since claims alone contradict the very definition of digital trust – i.e., *evidence based* confidence. This technique is also used when a private cloud is *not* sought as an answer. It appears to be most often applied by individuals and SMBs. In the case of presumptive security, the client believes that the cloud vendor “must” have better security than is provided locally (because the cloud vendor is often a big, experienced IT firm), so the absence of transparency is no longer a concern.

In some cases, this could be the equivalent of “diving to the bottom” – i.e., seeking whatever security is available rather than the digital trust that is needed to create enterprise value. The discourse over the use of this technique continues, with business and government eager to get beyond “security in the cloud” as an obstacle to its use. On the one hand, SMBs have declared the fears about cloud security to be “overblown,” and at least one survey of CIOs in the U.K. has dismissed cloud security concerns.⁶² On the other hand, another survey of CIOs in the same country found that 77 percent of respondents cited “security issues, uncertain reliability and concept immaturity” as reasons for *not* moving to cloud computing!⁶³ Other global surveys also show a reluctance to adopt cloud computing because of fears around security and control.⁶⁴ John Chambers, CEO of Cisco, has declared cloud computing to be a “security nightmare,” and a Forrester report declares that cloud security “demands greater scrutiny” than traditional outsourcing!⁶⁵ And so the discourse ping-pongs back and forth. Research and attempts at reconciling these competing claims also continue, with such



organizations as the Jericho Forum issuing a “Cloud Cube Model” whitepaper that suggests four dimensions for measuring or defining a cloud configuration and its suitability for use in specific circumstances.⁶⁶

Sometimes cloud service vendors can inadvertently confuse the claim circumstance by referring to their own processes, certifications, or broad attestations as support for “presumptive security.”⁶⁷ These can amount to no more than additional claims, unless the claim is accompanied by evidence to the user regarding the user’s own specific operation. For example, simply “having” a SAS70 audit performed is not the same as giving evidence of client policy compliance as a result of the SAS70. Cloud processing technology and service providers acknowledge the distinction and confirm that it is an obstacle. Speaking at an RSA conference panel in April 2009, Jian Zhen, director of cloud solutions at VMware, seemed to echo the industry awareness when he said, “It’s not that we don’t have better security – it’s just not enough transparency.”⁶⁸ Ironically, transparency is the only way of letting cloud processing users decide for themselves whether cloud providers really have “better security” or not, thereby generating digital trust. GE, in its use of Aravo’s SaaS product as described in Figure 8, resolved this digital trust need by performing *its own* audits of the service, looking specifically for the security characteristics GE desired and using that evidence to generate digital trust.

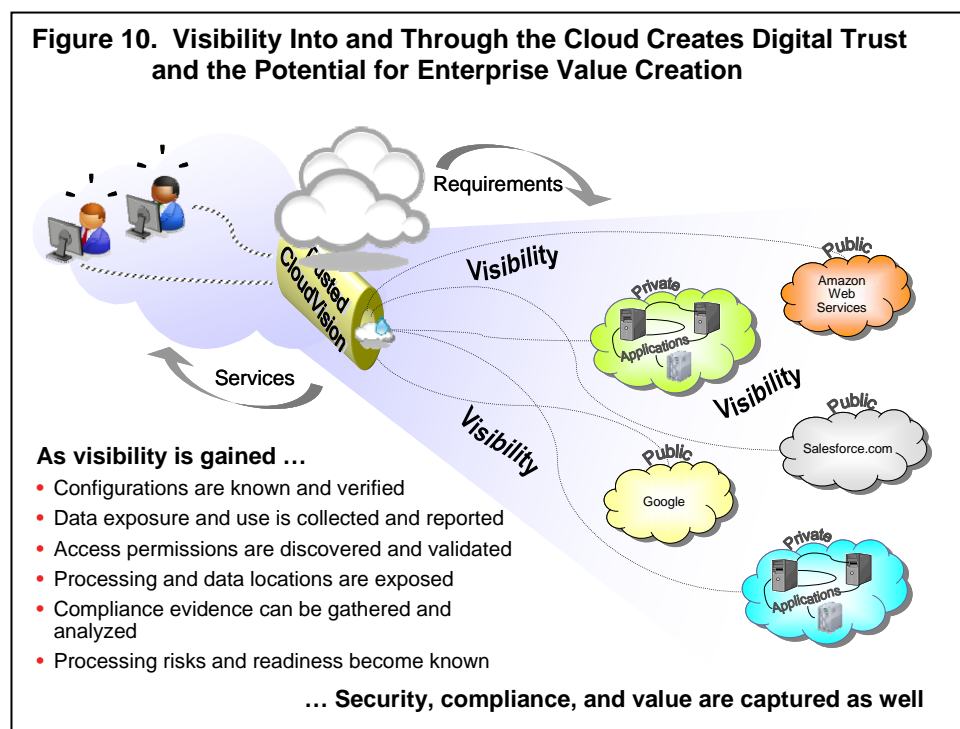
Claims alone are not sufficient to create digital trust. Evidence-based confidence is needed.



CSC Trusted Cloud Services: Liquid Security to Brighten the Cloud

So, what prevents an enterprise-scale explosion in cloud processing that matches the individual and SMB growth patterns that have already been recorded? What digital trust in cloud processing must be created so that the hesitation and constraints historically applied by enterprises to make cloud processing “safe” can be relaxed? How can we liberate organizations with digital trust in the cloud so that the promise of big payoffs with cloud processing can be realized by the enterprise? If we deliver answers to these questions, then cloud processing in all its styles can become available to the enterprise in far greater measure, and new value can be sought and captured.

For CSC, the answer lies in restoring visibility into and through the cloud. As illustrated in Figure 10, providing *visibility* in clouds increases *transparency*, and that transparency makes important *evidence* that can reinforce *customer confidence* and create *digital trust*. The greater the transparency, the greater the possibilities for evidence collection, and the more digital trust can be created. Ideally, working with a “glass cloud” would create the most digital trust and make the full elastic benefits of cloud processing available to the enterprise.



Cloud processing is a perfect scenario for the application of “liquid security” – i.e., “digital trust when time, place, and platform don’t matter”.⁵⁷ In cloud processing, “only the service matters.”⁶⁹ The whole idea is to abstract the application from the reality of hardware, software, and network configurations, and thereby value and buy as a service only what is needed (the application) and only when it is needed. This is precisely the stuff of liquid security, and it is on this basis that the security foundation of the CSC cloud computing initiative has been placed.

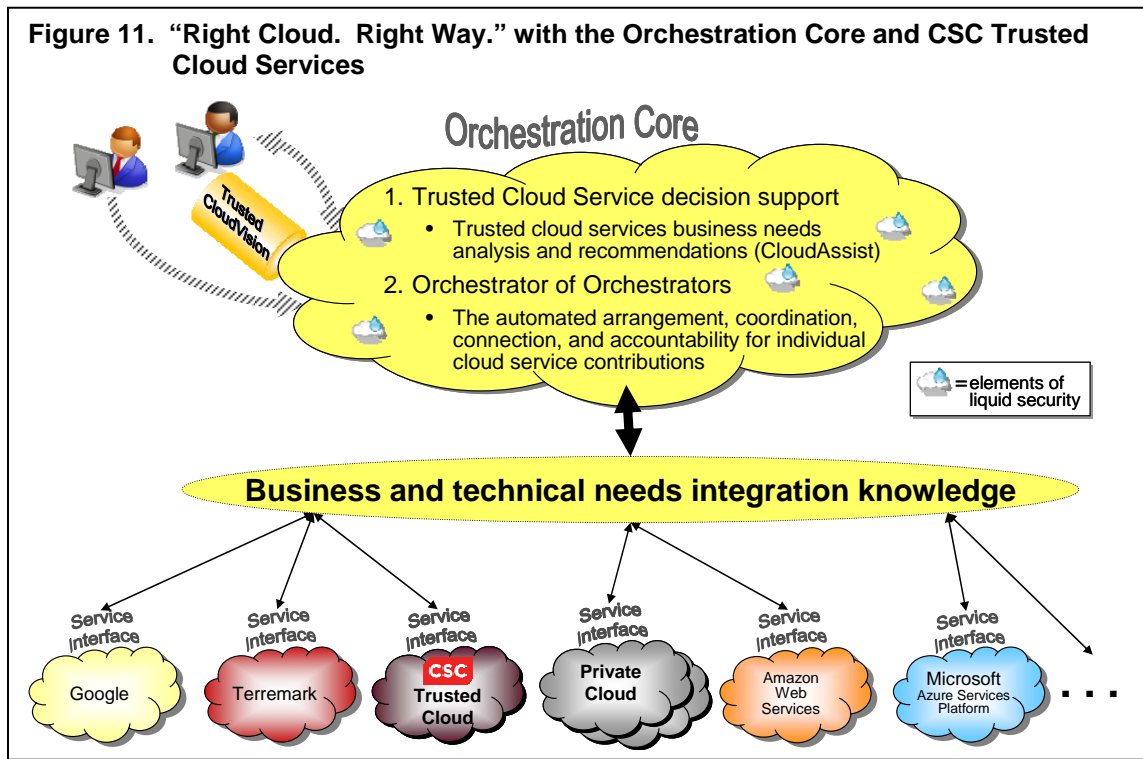
All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.



CSC Trusted CloudVision

CSC’s strategy for restoring visibility into and through cloud processing is known as “Trusted CloudVision.” In addition to a full business process, “best-of-breed” program and technology alliances, and a global effort to include customers and service partners in the definition and delivery of CSC cloud services, CSC Trusted CloudVision is provided through three primary activities, announced on June 1, 2009:⁷⁰

- *Cloud Orchestration Services* for heterogeneous cloud service integration and management, including the ability to request, retrieve, measure and report on elements of transparency from whatever cloud services might be engaged. As profiled in Figure 11, the CSC Cloud Orchestration Services provide two primary functions: (1) the translation of client enterprise business needs into alternative cloud service combinations – i.e., a *CloudAssist* function; and (2) the automated arrangement, coordination, connection, federation, management, security and operational accountability of cloud services of all styles, including the support of industry-specific compliance and auditing needs.
- *Trusted Cloud Services™* to provide a portfolio of industry-compliant desktop, computing, storage and network infrastructure services available on a just-in-time, on-demand basis, with full security features and stringent service-level criteria.
- *World Class Consulting Capabilities* to help enterprise information technology clients of all sizes and types take advantage of the best cloud processing capabilities for their own benefit.



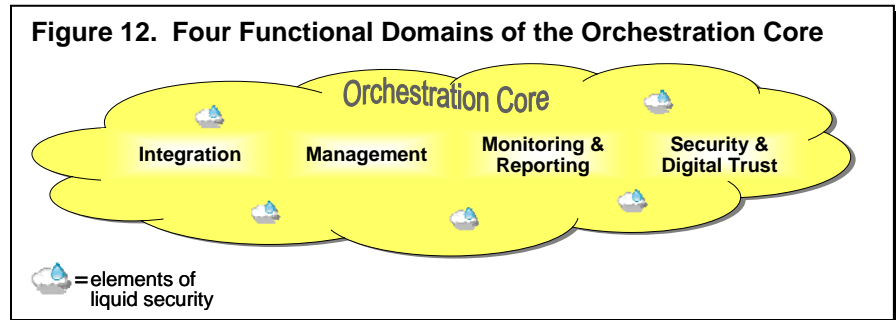
All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.



This three-way combination of activities delivers the right kind of information and help to clients so that the choice of cloud alternatives once again is reliably back in their hands. This is the “Right Cloud. Right Way” result targeted by CSC as illustrated in Figure 11.

The Orchestration Core (OC) provides the central organizational, connection, control and accountability service, using a variety of best-of-breed technologies and protocol foundations. Serving as an “orchestrator of orchestrators” across multiple cloud service points, the OC

executes in four important domains as identified in Figure 12: integration, management, monitoring and reporting, and security and digital trust. Throughout its operation, elements of liquid security⁵⁷ that help to re-establish



transparency into and through the various cloud servicing units (including the OC itself) are requested, collected, collated, and reported to clients and the CSC service teams.

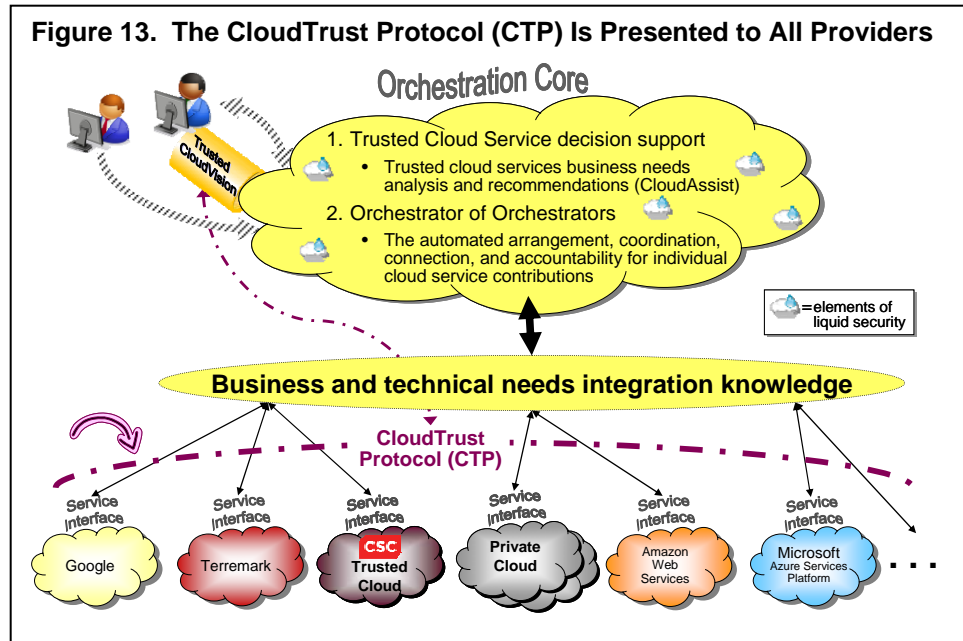
Since cloud processing service providers of almost any source (public or private) are candidates for delivering cloud services to a client, the *elements of transparency* (also called elements of liquid security) that are needed to provide evidence and generate or confirm digital trust must also come from those same varied sources. And, since the number of legitimate cloud service providers is likely to fluctuate over time, no single cloud service provider should be a priori excluded from delivering service to a client through the OC. So, how do we open the OC equally to all qualified cloud service providers without sacrificing the ability to collect, interpret, and report on the security and digital trust of that provider (either singly or in combination)?

This is the beginning of the CloudTrust Protocol (CTP).



CloudTrust Protocol (CTP)

The CloudTrust Protocol (CTP) is the mechanism by which the OC asks for and receives information about the elements of transparency that can be used to generate evidence and digital trust in the cloud processing that is being performed on behalf of a client. It is an asynchronous “question and response” protocol that is presented to all providers and is ultimately controlled by the clients themselves. Figure 13 shows the placement of the CTP in the organization between the OC and the various cloud processing service providers who are available to provide service, or who are already providing cloud service.



The CTP solves two client needs for security and trust in the cloud with one mechanism. First, it provides a way for clients to specify and ask about the

configuration, vulnerability, access, authorization, policy, accountability, anchoring, and operating status conditions *that they are really interested in*. Not every security issue is a concern for every client. Context is everything, and that context is known best by the client. This puts control (and decision making) back in the hands of the customer. Second, the CTP provides a way for cloud service providers to prepare and deliver information in response to requests about elements of transparency *in the best possible way for them*. Simply insisting on a (single) specific internal method or technique for all cloud service providers to use when they calculate or respond to an information request is self-defeating.

Cloud service providers can choose to respond or not respond to CTP requests. The ability to respond to different CTP requests is itself a measure of the *capacity to produce evidence* – i.e., the capacity to create digital trust and thereby enable value capture for the client enterprise. This measure is combined in the OC with other cloud service provider measures of things such as reputation, SLAs, service costs, service availability (including backup and restore capabilities), and standardization, and it is included in the OC calculations for the CloudAssist function and for ongoing expressions of the value of the cloud service being provided. By design, the CSC Trusted Cloud shown in Figure 13 will respond to all elements of the CTP.

All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.



Elements of Transparency

The elements of transparency included within the CTP continue to evolve. Figure 14 shows an outline of the current set of elements, divided into three types and multiple families. CSC is collaborating with NIST, the Object Management Group (OMG), current customers, and service partners to adjust and confirm the primary elements of transparency in the CTP.

Figure 14. Elements of Transparency Currently in CTP

Type	Family	Information Request or Delivery
Initiation	Identity / Session	<ol style="list-style-type: none"> 1. Identify service owner and initiate evidence session 2. Terminate evidence (CTP) session
Evidence Requests	Configuration	[for all cloud service units supporting service owner ...]
 SCAP 		3. What is current configuration for {Hypervisor? Guest O/Ss? Virtual switches? Virtual firewalls? IDS?}
		4. How does current configuration of {service unit type} differ from {service owner configuration specification/policy}
	Vulnerability	[for all cloud service units supporting service owner ...]
		5. Results of latest vulnerability assessment on {hypervisor; guest O/Ss; virtual switches; virtual firewalls}
		6. Date of latest vulnerability assessment on {hypervisor; guest O/Ss; virtual switches; virtual firewalls}
		7. Perform vulnerability assessment now on {hypervisor; guest O/Ss; virtual switches; virtual firewalls}
	Anchoring	[for all cloud service units supporting service owner ...]
		8. Provide geographic location and affirmation (by unit identity)
		9. Provide platform separation affirmation and identities (by unit identity)
		10. Provide process separation affirmation – positive or negative – (by process name – e.g., storage encryption, storage de-duplication, backup, ...)
	Audit Log	[for all cloud service units supporting service owner ...]
		11. Provide log of policy violations {in last 'n' hours} (e.g., malware elimination, unauthorized access attempts, ...)
		12. Provide audit/event log {for last 'n' hours}
		13. Provide list of currently authorized users/subjects and their permissions
		14. Provide incident declaration and response summary {for last 'n' hours}
	Service Management	[for all cloud service units supporting service owner ...]
		15. Provide indicator/record of changes made and/or changes requested but not made (change control / configuration control)
Policy Introduction	Users & Permissions	16. Provide declaration of user types, permissions, and provisioning/de-provisioning sources
	Configurations	[for all cloud service units supporting service owner ...]

All rights reserved. This document is a proprietary product of CSC and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission CSC, is strictly prohibited.



Figure 14. Elements of Transparency Currently in CTP

Type	Family	Information Request or Delivery
SCAP→		17. Provide configuration standards to be applied (SCAP/CCE)
	Anchoring	18. Provide anchoring needs for geographic, process, and platform anchoring
	Quotas	[for all cloud service units supporting service owner ...]
		19. Provide quotas for use

Figure 14 is a only a sketch of the CTP. Technical formats and request/response delivery mechanisms are still in development. In the simplest designs, email can be used as the transport mechanism for the CTP elements. Nevertheless, for at least some of the elements in the CTP, a ready-made protocol foundation already exists. The Security Content Automation Protocol (SCAP)⁷¹ provides a proven method for the enumeration of configurations and vulnerabilities and for measuring differences between requested configurations and those being used. So, elements in the “Evidence Requests” and “Policy Introduction” types of CTP are natural candidates to be expressed and relayed and responded to through SCAP. As SCAP extensions emerge,⁷² then even more of the elements of the CTP can be automated through the standard, and more transparency (and digital trust) can be created more easily. For instance, the Open Checklist Interactive Language (OCIL) and the Open Checklist Reporting Language (OCRL)⁷³ are both promising efforts that would further automate some of the transparency element interactions of the CTP in the Orchestration Core.

Not all of the CTP elements of transparency need be used every time. For example, quotas or configurations may not be necessary for certain clients. In those cases, simply leaving them out is just fine. The basis of the CTP is not to encumber cloud users with needless information inputs and exchanges. Rather, it is to make elements of transparency that are meaningful to the client available as evidence, and to combine that evidence on behalf of that client to help create digital trust. In the end, that digital trust creates enterprise value for the client. Once again, “Right cloud. Right way.”



CSC Trusted Cloud Services at Work

Imagine this:

You are the managing partner of a 20-doctor medical practice in the Midwest U.S. Your successful practice “went public” a few years ago and is a “for profit” enterprise on behalf of its shareholders. All but two of your practice doctors are general practitioners. The others are pediatricians. You maintain a service and accredited staff relationship with three different hospitals and clinics in two different states. It is your practice policy to accept Medicare and Medicaid for payment, but only if the patient has presented a major credit card to take care of any deductibles.

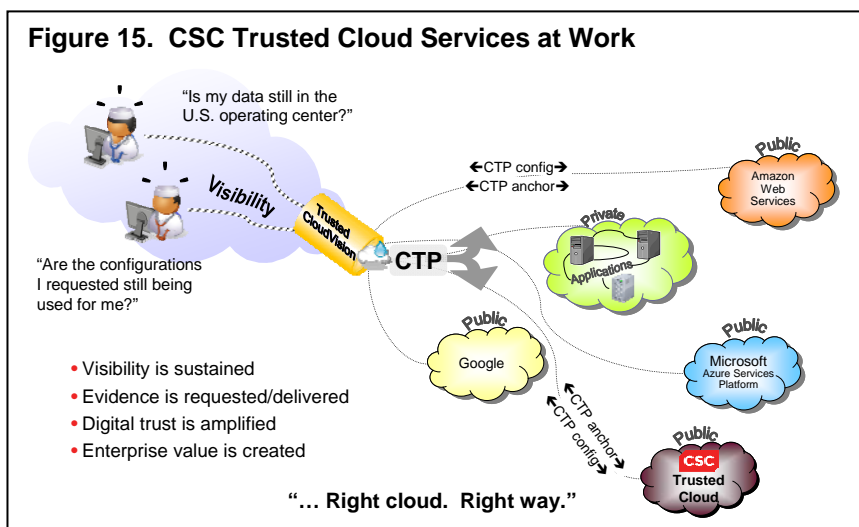
You have been running your own practice automation system that you licensed from a software vendor. It includes a form of electronic patient health records, but it has not been certified to U.S. Department of Health and Human Services standards. Your practice does undergo independent audits. Your controls plan (in support of audits) depends on having specific configurations of the equipments in use in order to make claims of control for the information technology.

Two years ago you went to email and word processing “as-a-service.” You now wish to take advantage of incentives offered in the American Reinvestment and Recovery Act of 2009 (ARRA) and move to a fully certified electronic patient record system. Your practice analysis has shown that if you evolve all the way to “medical practice-as-a-service,” you will be able to double your practice size while reducing your patient wait times and liberating your practice doctors to spend 12 percent more time with each patient. This represents an enormous competitive advantage and would generate new value for your medical practice enterprise.

Can you do this?

CSC Trusted Cloud Services with the Orchestration Core and Trusted CloudVision can respond to this kind of scenario and help capture the enterprise value sought by the medical practice. Figure 15 illustrates how the functions of Trusted CloudVision help to bring the kinds of visibility to the practice that is needed to satisfy the web of security and compliance obligations.

In particular, we can see examples of the CTP being used to request and receive evidence that necessary conditions for secure and compliant operation are being followed.





How does CSC Trusted Cloud Services work for the sample scenario of the medical practice?

- The CloudAssist function (using a combination of the specialist global consulting practice and the automated analytical support of the Orchestration Core) helps the client identify which combination of cloud service providers are capable of delivering the compute and storage services needed *along with* acceptable levels of reliability, cost, reputation, and SLAs, as well as the necessary transparency.
- The transparency needs (to generate digital trust) are derived from two basic sources. First, regulatory mandates from the Health Insurance Portability and Accountability Act (HIPAA), the Centers for Medicare & Medicaid Services (CMS), Sarbanes-Oxley, and the Payment Card Industry Data Security Standard (PCI DSS) automatically apply. Then, reporting for the investment of the ARRA funds is added to this initial obligation, plus whatever compliance evidence is needed by the associated hospitals and (multi) state regulators.
 - HIPAA and CMS have both security and privacy obligations. Encryption of patient data (in transit and in storage) is essential, as is a backup repository. This is an example of “process anchoring” – i.e., anchored to an encryption process.
 - Sarbanes-Oxley requires a level of controls visibility to make sure that the financial results being reported by the practice are indeed accurate. IT controls on data location, access, auditing, and monitoring are needed in a formal controls plan.
 - PCI DSS requires some separation of payment card application processing from the database of payment card data. This is “platform anchoring” – i.e., an applications process anchored apart from the database process.
 - Although U.S. patient data would not automatically be required to be stored in U.S. locations, the example medical practice prefers that option. This is an example of “geographic anchoring” – i.e., processing and data anchored to equipment and facilities located in the U.S. ITAR-designated data would require such anchoring.⁷⁴

Clearly, a cloud provider's SAS70 is not enough ... even if it were provided to the medical practice!

- Once a combination of public cloud, private cloud, and managed service capabilities has been chosen, the Orchestration Core is used to arrange, organize, connect, monitor, and manage all of the services being used, ultimately providing one service interface to the client. Services are started and stopped to match need. A single help desk responds to all issues. All services are monitored and metered. One bill is generated. And, throughout the day-to-day operations, medical practice staff (and CSC administrators) can use the transparency provided by Trusted CloudVision and the CTP to request and receive evidence of policy compliance when needed. Every time the evidence is provided, digital trust is displayed and increased, and value is captured.

This is digital trust in the cloud.



The Last Word

So far, the debate is endless. Are we at the fraying ends of a fad, or the beginning of a bonanza of IT value and performance? It seems as if *everybody* wants to put *something* into the cloud, but *nobody* wants to put *everything* into the cloud! Are we about to embark on a stream of business IT spending growth on cloud services that IDC predicts will rise to \$42 billion by 2012?⁷⁵ Or, is the situation exactly as the infamous “Mafiaboy” has declared: “Cloud computing will cause an Internet security meltdown!”⁷⁶ The end of the story is not yet known. But, there are some important digital trust conclusions to draw with the information and evidence that is at hand:

- Secure cloud processing *must* offer more than just economy. Otherwise, the promise of elastic benefits will not be realized or sustained, and “cloud” processing will soon be replaced by new metaphors for IT processing ubiquity and convenience. Consequently, “security” in the cloud is not enough. “Trust in the cloud” is necessary to create new enterprise value.
- Public or community clouds organized vertically around single industry needs or horizontally against specific functions seem easiest to explain and offer. Their security needs can be constrained by scope of service, so their transparency and digital trust delivery can be smaller. As a consequence, they likewise appear to have the simplest path to initial growth.

For example, the track record of Salesforce.com as the “CRM-as-a-service” provider of choice for millions is the most obvious evidence. But, health care clouds like RevolutionHealth and Microsoft’s HealthVault already have a “healthy” following (if not stunning financial rewards).⁷⁷ With the emphasis on health care and the amount of funding (government and commercial) involved, even more cloud service providers are trying to claim some space in this vertical. Amazon, for instance, now offers a whitepaper on how to create HIPAA-compliant information processing systems in the AWS cloud.⁷⁸

Today we find clouds for other industries and professions emerging as well. A “legal cloud” has already been announced by nScaled,⁷⁹ and we can expect similar offerings for verticals like finance and agriculture. Likewise, horizontally targeted clouds like Skytap’s application development and testing cloud⁸⁰ and Datacastle’s enterprise PC backup and restore cloud⁸¹ target service needs whose transparency and digital trust needs can be met today. Even “security as a service” is available from companies like McAfee, F-Secure, and Panda Security.

- There is no shortage of research efforts, study programs, and consortia of all kinds trying to provide advice, structure, and clarity to the discipline of cloud processing, and in particular the security and privacy issues surrounding cloud processing. In addition to the well-known and advertised efforts of such bodies as NIST, the OMG, and the Cloud Security Alliance (CSA), many other global and regional organizations are also hard at work. The European Union, universities the world over, government and commercial research units, the World Privacy Forum, the Open Grid Forum, the Open Cloud Consortium, and countless others are investigating the way clouds are best defined and



operated. Some have even argued for a stamp of certification, like a “kite mark” system, to improve the security credentials of cloud processing.⁸² Many publications, conferences, commentaries, reports, and blogs are released with the hope of improving the status quo for cloud processing. With so much going on, we can paraphrase an old saying that applies: “It’s hard to see the weather front for the individual clouds.” Embedded in all of this is the need for digital trust in the cloud.

The realization of enterprise benefits from the elastic nature of cloud processing is perhaps the biggest (potential) digital trust payoff ever. Think of it! Enterprises liberated to use cloud processing without hesitation. Big deeds with important applications providing huge payoffs not only in cost reduction, but in such things as increased revenue, new market access, reduced time to market, improved sales conversion rates, repackaging and reuse of existing intellectual property, faster and more accurate customer and citizen service, improved productivity (doing *more* for less), efficiency (doing *more* in less time), greater market share, and competitive advantage. These are results that make a difference to the enterprise. And digital trust in the cloud is the difference that can make these results possible.

So, resist the temptation to jump into even a so-called “secure” cloud just to save money. Aim higher! Jump into the right “trusted” cloud to create and capture new enterprise value.

Things are “looking up”!



¹ www.mortonsalt.com/heritage/heritage_timeline.html

² Reference definitions from all types of origins abound. For example:

- "Toward a Unified Ontology of Cloud Computing," Lamia Youseff, University of California, Santa Barbara (UCSB), with Maria Butrico and Dilma Da Silva, IBM, T.J. Watson Research Center, www.cs.ucsb.edu/~l:youseff/CCOntology/CloudOntology.pdf
- "Above the Clouds: A Berkeley View of Cloud Computing," Michael Armbrust et alia, Electric Engineering and Computer Sciences, University of California at Berkeley, 10 February 2009, www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html
- "How to Identify Cloud Computing," Darryl C. Plummer, Gartner Research, ID Number: G00158761, 24 June 2008, www.gartner.com/DisplayDocument?id=705817 (registration and membership required)
- "Future View: The New Tech Ecosystems Of Cloud, Cloud Services, And Cloud Computing," Forrester Report, Frank E. Gillett with Eric G. Brown, James Staten, and Christina Lee, 28 August 2008, www.forrester.com/Research/Document/Excerpt/0,7211,45073,00.html (full report requires purchase or client enrollment)
- "Computing Heads for the Clouds," Aaron Ricadela, *BusinessWeek*, 16 November 2007, www.businessweek.com/technology/content/nov2007/tc20071116_379585.htm
- "Security Guidance for Critical Areas of Focus in Cloud Computing," Cloud Security Alliance (not a specific definition, but an outline introducing a portfolio of domains in "Principal Characteristics of Cloud Computing"), April 2009, www.cloudsecurityalliance.org/guidance/csaguide/pdf
- "Microsoft unveils 'Azure' – its cloud computing vision," 28 October 2008, <http://searchcio.techtarget.com.au/articles/27489-Microsoft-unveils-Azure-its-cloud-computing-vision>
- "Enterprise 2.0: Google, Amazon, Salesforce Push 'Cloud' Vision," 10 June 2008, www.informationweek.com/news/hardware/utility_ondemand/showArticle.jhtml?articleID=208403130
- "Effectively and Securely Using the Cloud Computing Paradigm," Peter Mell and Tim Grance, NIST, Information Technology Laboratory, http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-pmell-day3_cloud-computing.pdf (see page 7 entitled "A Working Definition of Cloud Computing"). Also, see a different definition in "Perspectives on Cloud Computing and Standards" http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-standards_ISPAB-Dec2008_P-Mell.pdf
- "Guide to Cloud Computing," Richard Martin and J. Nicholas Hoover, *Information Week*, 21 June 2008, www.informationweek.com/news/services/hosted_apps/showArticle.jhtml?articleID=208700713
- The McKinsey & Co. Report "Clearing the Air on Cloud Computing" has stirred quite a debate on its methodology of analysis and its conclusions. However, this report also notes a recent academic study that identified 22 definitions of cloud computing in common use. See www.computerworld.com.au/article/300901/mckinsey_cloud_computing_report_conclusions_don_t_add_up for a review of the report. For the entire report, see <http://uptimeinstitute.org/content/view/353/319> (membership required).

³ www.dfinews.com/articles.php?pid=389

⁴ Information Technology (IT) is not the only resource that has been projected to have "elastic" benefits and payoffs in the future. For a more complete discussion of resource elasticity, see "Everything Elastic" at www.cio.com/documents/whitepapers/accnturevisionwp.pdf.



⁵ See Table 1 on page 3 of “Above the Clouds: A Berkeley View of Cloud Computing,” Michael Armbrust et alia, Electric Engineering and Computer Sciences, University of California at Berkeley, 10 February 2009, www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

⁶ See the interview with Ray Ozzie at www.informationweek.com/news/showArticle.jhtml?articleID=211800091

⁷ www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=330039

⁸ “Cloud Control”, www.internetevolution.com/document.asp?doc_id=170782&. There are other thoughtful attempts to identify reasons why enterprises continue to hesitate in their adoption of cloud processing. For instance InfoWorld reported in 2008 on a Gartner report that listed seven “cloud computing risks” as hindrances to the wider use of cloud processing. According to the report, those seven risks included the security concerns of privileged access, regulatory compliance, data location, data segregation, disaster recovery, investigative support, and long-term viability. See a synopsis of the report at www.infoworld.com/article/08/07/02/Gartner_Seven_cloudcomputing_security_risks_1.html or purchase the entire report at www.gartner.com/DisplayDocument?id=685308.

⁹ For a full definition and explanation of why transparency is a root source of digital trust, see “The Completion of Digital Trust” (p. 3) in Volume 1 of the *Digital Trust* research report, “Digital Trust: Shaking Hands with the Digital Enterprise,” part of an eight-volume report published by CSC’s Leading EdgeForum, 28 June 2007, www.csc.com/aboutus/leadingedgeforum/knowledgelibrary/uploads/LEFReports2007_DigitalTrustVol1.pdf
(All report volumes can be found at <http://www.csc.com/lefreports>)

¹⁰ See, for example, the Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, of the American Institute of Certified Public Accountants (AICPA). A SAS 70, Type II audit includes tests by the independent service auditor of the operating effectiveness of the (claimed) IT controls (www.sas70.com/about.htm#about%20100). With no visibility through the cloud, independent verification is stymied.

¹¹ For an introductory discussion of digital trust payoffs and penalties, see “Where Does Digital Trust Come From?” in Volume 1 of the *Digital Trust* research report, “Digital Trust: Shaking Hands with the Digital Enterprise,” pp. 10-11, www.csc.com/aboutus/leadingedgeforum/knowledgelibrary/uploads/LEFReports2007_DigitalTrustVol1.pdf

¹² Virtualization is certainly not a requirement for “private clouds.” For example, the U.S. Department of Veterans Affairs has deployed a small internal cloud using PAN Manager from Egenera (www.egenera.com). PAN Manager can move workloads around without benefit of hypervisor software. (From “Private Clouds on the Horizon,” Information Week Analytics, 13 April 2009, pp. 2-5, http://i.cmpnet.com/informationweekreports/doc/2009/InformationWeek_Analytics_Alert_PrivateCloud.pdf, registration required)

¹³ For instance, Google uses a different abstraction technique in order to achieve its cost, integrity, and availability targets. See, for example, http://news.cnet.com/Googles-secret-of-success-Dealing-with-failure---page-2/2100-1032_3-5596811-2.html?tag=mncol or www.virtualization.info/2005/12/will-google-embrace-virtualization.html or www.theregister.co.uk/2007/06/25/google_barroso_datacenter/. For a complete discussion of the Google architecture that emphasizes replication and redundancy, view the University of Washington CSE Colloquium lecture from 2005 at <http://www.uwv.org/programs/displayevent.aspx?rID=3898>. This is a long video, but it has a very comprehensive discussion of the Google emphasis on building reliable services from lots of unreliable



parts. The use of replication, redundancy and parallelism is at the heart of the Google abstraction (rather than conventional virtualization).

¹⁴ www.itbusinessedge.com/cm/community/features/articles/blog/better-together-virtualization-and-the-cloud/?cs=23204

¹⁵ www.infoworld.com/d/virtualization/vendors-air-clouds-pros-and-cons-004

¹⁶ <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v14.doc>

¹⁷ “Executive Summary,” NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, p. 1, <http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>. For a copy of OMB A-130, see www.whitehouse.gov/omb/circulars_a130_a130trans4/.

¹⁸ <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

¹⁹ www.nist.org/nist_plugins/content/content.php?content.16

²⁰ Adapted from “Figure 1: The Risk Management Framework” of NIST Special Publication 800-53, Revision 1, p. 16, <http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf>. The chart is also available from a NIST briefing available at www.hq.nasa.gov/office/oig/hq/ITR/presentation020204-1.ppt and from a briefing on the NIST Security Certification and Accreditation Project by Dr. Ron Ross, http://archive.opengroup.org/public/member/proceedings/q403/evm_ross.pdf, p. 9.

²¹ www.dtic.mil/whs/directives/corres/pdf/851001p.pdf

²² Available at www.dtic.mil/whs/directives/corres/pdf/850002p.pdf

²³ Uniformity of C&A process does not yet reign in the U.S. Notwithstanding the endorsement of the DIACAP in DoD, there remain C&A efforts following the (now superseded) Defense Information Technology System Certification and Accreditation Process (DITSCAP), two variants of the DCID 6/3 process, the DOD Intelligence Information Systems (DODIIS) Security Certification and Accreditation Guide, and the Joint DODIIS/Cryptologic SCI Information Systems Security Standards.

²⁴ The general notion of following a risk management process leading up to the preparation of “accreditation document sets” is followed in commercial and government standards. For example, in the United Kingdom, BS7799 (ISO17799 and now ISO27001) is invoked for “small government systems, local authorities and other non-governmental organizations that need to connect to Government Systems.” (<http://archive.cabinetoffice.gov.uk/e-envoy/resources-word/sfile/ISPD.doc>) In addition, HMG Infosec Standard 2 defines an accreditation document set that is to be used for complex systems in the U.K. (Along with the Manual of Protective Security (MPS), other HMG Infosec Standards describe the entire risk management process for the U.K. government, in a fashion similar to that provided by NIST and the DoD in the U.S.) See www.cpni.gov.uk/docs/re-20050804-00653.pdf. Other countries have equivalent frameworks.

²⁵ See the section entitled “The Fundamentals” in NIST Special Publication 800-53, Revision 3. <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>

²⁶ www.ucdmc.ucdavis.edu/compliance/guidance/privacy/penalties.html

²⁷ www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1205923895814



²⁸ See *The Federal Information Manual, How the Government Collects, Manages, and Discloses Information under FOIA and Other Statutes*, by P. Stephen Gidiere, American Bar Association, 2006. In particular, examine “SECTION 4.4 PENALTIES FOR UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION”, pp. 107 and following, for a listing and discussion of the federal statutes that prohibit the disclosure of all types of classified information.

²⁹ http://news.cnet.com/8301-17938_105-9721429-1.jhtml

³⁰ http://news.cnet.com/8301-1009_3-10014150-83.html

³¹ http://news.yahoo.com/s/ap/20090708/ap_on_re_as/as_skorea_cyber_attack

³² www.boston.com/news/nation/articles/2009/06/28/us_russia_disagree_on_cyberspace_treaty

³³ www.nextgov.com/the_basics/tb_20090601_8569.php

³⁴ See panel 10 of the briefing by Pete Verga, then the Principal Deputy ASD (HD&ASA), at the 2008 Defense Industrial Base – Critical Infrastructure Protection Conference in Miami, Florida, 7-9 April 2008, www.dtic.mil/ndia/2008dib_cip/Verga.pdf

³⁵ www.defence.gov.au/dmo/news/ontarget/oct06/hl3.cfm

³⁶ www.culture.gov.uk/what_we_do/broadcasting/6216.aspx (See Chapter 7, “Digital Security and Safety.”)

³⁷ http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf

³⁸ More description can be found at www.informationweek.com/story/showArticle.jhtml?articleID=218400025

³⁹ www.on-demandenterprise.com/topic/datacenter/DISA_CIO_Cloud_Computing_Something_We_Absolutely_Have_to_Do_31270309.html

⁴⁰ www.informationweek.com/story/showArticle.jhtml?articleID=218501405

⁴¹ “Private Clouds on the Horizon,” Information Week Analytics, 13 April 2009, p. 2-5, http://i.cmpnet.com/informationweekreports/doc/2009/InformationWeek_Analytics_Alert_PrivateCloud.pdf, (registration required)

⁴² See <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v14.doc> for the latest U.S. government (NIST) draft working definition of cloud computing.

⁴³ See “Weatherproofing the Cloud to Provide Some Digital Trust” on p. 21 for a list of the basic techniques being applied to overcome the absence of digital trust (the lack of transparency) in contemporary clouds.

⁴⁴ www.informationweek.com/news/showArticle.jhtml?articleID=218500656

⁴⁵ <http://cio.energy.gov/CloudComputing.htm>



⁴⁶ www.washingtonpost.com/wp-dyn/content/article/2009/03/30/AR2009033002848.html Also, Google claims to be working to obtain FISMA certification and accreditation for its services by the end of 2009 according to www.informationweek.com/news/showArticle.jhtml?articleID=218500656

⁴⁷ www.techflash.com/A_look_at_Amazons_government_cloud_strategy_45817132.html

⁴⁸ www.informationweek.com/story/showArticle.jhtml?articleID=217300737

⁴⁹ <http://au.sys-con.com/node/907744>

⁵⁰ www.informationweek.com/news/services/hosted_apps/showArticle.jhtml?articleID=217600423

⁵¹ www.itpro.co.uk/611947/government-cio-moots-g-cloud-app-store-plans

⁵² The traditional business case for SMBs and cloud processing is outlined in www.infosysblogs.com/cloudcomputing/2009/07/catalyzing_enterprenuership_1.html. A Forrester market assessment reached a conclusion that disputed this “conventional wisdom,” and that differing opinion is outlined in <http://business-technology-roundtable.blogspot.com/2009/06/demand-for-cloud-infrastructure-as.html> But, conventional wisdom remains that SMBs are the early and current drivers for cloud processing services.

⁵³ <http://community.citrix.com/blogs/citrite/scottsw/2009/06/25/Cloud+Computing+-+Private+and+Public>

⁵⁴ Based on a conversation between the author of this report (Ron Knode) and Jim Moran, the CISO at ETS, on 13 May 2009.

⁵⁵ Based on a conversation between the author of this report (Ron Knode) and Towson University system administrators on 21 July 2009. The author is also an adjunct faculty member at Towson University.

⁵⁶ Much of the material for this case study is from “Cloud Computing to the Max at Bechtel,” www.cio.com/article/453214. Some additional detail can be found at “Bechtel Harnesses the Cloud: Case Study of an Enterprise Cloud,” <http://cloudstoragestrategy.com/2009/03/bechtel-harnesses-the-cloud-a-case-study-in-service-delivery.html>

⁵⁷ For a discussion of digital trust as “liquid security,” see Volume 5 of the *Digital Trust* report series, “Liquid Security – Digital Trust When Time, Place and Platform Don’t Matter,” CSC Leading Edge Forum,, 25 September 2007, www.csc.com/aboutus/leadingedgeforum/knowledgelibrary/uploads/LEF_2007DigitalTrustVol5.pdf

⁵⁸ J. Nicholas Hoover, “GE Tests Private Cloud Model,” *Private Clouds on the Horizon*, Information Week Analytics, April 13, 2009, pp. 9-11, http://i.cmpnet.com/informationweekreports/doc/2009/InformationWeek_Analytics_Alert_PrivateCloud.pdf

⁵⁹ http://www.businessweek.com/technology/technology_at_work/archives/2009/05/tk_google_apps.html

⁶⁰ www.itworld.com/saas/61383/ge-gets-cloud-new-saas-supply-chain-app

⁶¹ Gartner’s estimate of global IT spend is down 6 percent in 2009 from 2008 but still totals \$3.2 trillion. https://news.fidelity.com/news/news.jhtml?cat=Tech&articleid=200907070636RTRSNEWSCOMBINED_BOM14518_1&IMG=N



⁶² “Cloud security fears called overblown, ‘emotional’ at IDC forum” (www.computerworld.com/s/article/9128260), “Businesses dismiss cloud security concerns” (www.networkworld.com/news/2009/071709-businesses-dismiss-cloud-security.html)

⁶³ www.informationweek.com/story/showArticle.jhtml?articleID=217800162

⁶⁴ Two recent global surveys that show a hesitancy to adopt cloud processing due to security can be retrieved at www.infoworld.com/d/cloud-computing/survey-casts-doubt-cloud-adoption-274 and at www.marketwire.com/press-release/Avanade-953525.html

⁶⁵ “Cloud security demands greater scrutiny than traditional IT outsourcing, Forrester says,” www.networkworld.com/news/2009/051109-forrester-cloud-security.html, and “Cloud computing a ‘security nightmare,’ says Cisco CEO,” www.networkworld.com/news/2009/042309-cloud-computing-a-security-nightmare.html

⁶⁶ www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

⁶⁷ See, for example, “Securing Microsoft’s Cloud Infrastructure,” May 2009, p. 15, wherein Microsoft (rightly) expresses its *commitment* to delivering a “trustworthy cloud computing infrastructure” by *having* an ISO/IEC 27001:2005 certificate and SAS70 audits. While praiseworthy, these items do not automatically constitute evidence for a particular client and a particular use of the cloud. www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf

⁶⁸ www.darkreading.com/securityservices/security/management/showArticle.jhtml?articleID=217702062

⁶⁹ This is the cloud version of the phrase, “Eventually, the only thing that matters is the application itself.” From Volume 5 of the *Digital Trust* report series, “Liquid Security – Digital Trust When Time, Place and Platform Don’t Matter,” CSC Leading Edge Forum, 25 September 2007, www.csc.com/aboutus/leadingedgeforum/knowledgeibrary/uploads/LEF_2007DigitalTrustVol5.pdf, p. 5.

⁷⁰ www.csc.com/newsroom/press_releases/27446-csc_announces_new_family_of_cloud_services

⁷¹ <http://scap.nist.gov/index.html>

⁷² <http://scap.nist.gov/emerging-specs/listing.html>

⁷³ <http://ocrl.mitre.org>

⁷⁴ International Traffic in Arms Regulations (ITAR). A set of United States government regulations that control the export and import of defense-related articles and services on the United States Munitions List. Other countries have equivalent sets of regulations and requirements.

⁷⁵ www.technologyreview.com/read_article.aspx?id=22605

⁷⁶ www.darkreading.com/securityservices/security/attacks/showArticle.jhtml?articleID=218102139

⁷⁷ See www.revolutionhealth.com and www.healthvault.com. For a commentary on the digital trust impact and value for such health portals (health clouds), see the CSC digital trust blog by Ron Knode at www.csc.com/ee/lef/C9/P10.

⁷⁸ http://awsmedia.s3.amazonaws.com/AWS_HIPAA_Whitepaper_Final.pdf

⁷⁹ <http://cloudsecurity.org/2009/05/08/legal-cloud-have-it-your-way/>



⁸⁰ www.skytap.com

⁸¹ www.datacastlecorp.com

⁸² www.v3.co.uk/2244732