

ACS’ ITO Perspective on Cloud Computing:

“Putting People Back In Cloud”

An ACS White Paper



A **xerox**  Company

Chris Mankle
May 2010



A **xerox**  Company

ACS is now a Xerox company

Putting People Back In Cloud

Cloud computing has dominated blogs, conferences and the minds of CIOs around the world in recent days, bringing the promise of agility, scalability, and cost advantages to waiting markets. Although nearly all potential users can see the benefits of the concept, one key issue is slowing or preventing more from jumping on board. Even a partial transition from a tangible, visible world into a multi-tenant virtual environment can feel more like a leap of faith than a viable business decision. Users want to know that their processes will continue to function, that their data will be protected and kept confidential, and that they will still have the same level of governance in the widespread, data-everywhere cloud environment as they do in the data center next door. They have contracts, assurances, and descriptions of a litany of tools designed to protect data, promote confidentiality, and audit performance. Still something is missing.

That something is *trust*.

Countless papers have been written on hypervisor firewalls, redundancy, and cloud computing technology itself, yet the fear factor remains unchanged. ACS has a different perspective on building trust in the virtual world. In our minds, although the security safeguards and base technology are vitally important, no one really trusts a computer or a cloud. Even in the virtual world, it all comes down to people making the computers, networks, and storage solutions work. So the question becomes not “what will make you trust cloud,” but rather, “who do you trust to manage your cloud environment on your behalf?”

Assigning Trust is a Scientific Process

By definition, trust is reliance on the integrity or justice of a person, or confidence in some quality, feature or attribute of a person or thing; a person on which one relies. Although it may feel instinctual, trust is something most human beings are conditioned to assess, based on context and other factors, in what has proven to be a very scientific way.

Let’s step outside of cloud into real, everyday life for a moment. You’re at home and someone comes to your door and knocks. How you react depends on what you see when you look out of the peephole.

For example, if you see a good friend, you’ll probably swing open the door and invite him or her in. If you see a neighborhood kid selling popcorn or the UPS delivery person with that e-reader you’ve been waiting for, you’ll probably open the door without trepidation. Chances are you’ll react differently if you see someone you don’t recognize at your door. Maybe you’ll open the door with the safety latch on – or not open the door at all. Now, if that stranger is standing there with a bouquet of flowers, and there’s a delivery van emblazoned with the logo of a local florist visibly parked on the street, you’ll have a different reaction still.

Trust isn’t stagnant. It’s something that’s continually accessed and built over time, and also something that can be lost in an instant. For example, let’s say you’re looking for a great new restaurant. You might look at the newspaper, some on-line reviews or seek out the recommendation of a co-worker whose culinary opinion you trust. A good experience builds trust and keeps you coming back. But, if one night, that now-favorite restaurant becomes the cause of food poisoning, the trust quickly diminishes or disappears.

In your personal world and in the business world, there is a direct correlation between trust and risk. Going back to the stranger at the door example, if that person is standing there with a delivery or floral arrangement, you’ll probably assign a lower risk level to the situation than if there’s a stranger at the door, standing there empty-handed.

When CIOs look at cloud computing, they see that stranger at the door – the potential for risk. So, after looking at the background, track record and approach of potential cloud services providers, the deciding factor has to come down to who has the capability to best manage your risk in the cloud environment? That’s the provider you can trust to transform your organization into a cloud.

Applying ISO31000 to Risk Management

Although we manage risk instinctively on a daily basis, on the enterprise level, effective risk management is based on standardization and some distinct processes designed to mitigate unfavorable outcome.

In November 2009, the International Organization for Standardization (ISO) published *ISO 31000:2009, Risk Management -- Principles and Guidelines*, a new management standard intended to help organizations of all types and sizes manage risk across the enterprise. It provides a generic framework for establishing the context of, identifying, analyzing, evaluating, treating, monitoring, and communicating risk. Essentially, it focuses the risk management process into a series of the following coordinated activities:

Establishing the context – just as there are different risk factors for the stranger at your door versus the stranger who is following a little too closely on the street, there are different risk factors for private and public clouds. Does your provider recognize the difference in its approach to security, visibility, awareness, and operations?

Risk identification – recognizing the risk is the first step to mitigating it. Does the provider have a means to actively find, recognize, and describe the potential risks in your specific cloud model?

Risk analysis – does your provider have a means of delving deeper into the nature of the risk and ranking its potential harm level?

Risk evaluation – at this point, the provider should be able to compare the results of the risk analysis with the established risk criteria to determine whether the magnitude of potential risk is acceptable.

Risk treatment – is there a way to modify or nullify the risk before going forward?

Communication and consultation – ongoing communications with stakeholders about potential risks, treatments, and next steps are critical to both mitigating risk and building trust. The risk management process relies on continual information exchange and provider-client dialogue.

Monitoring and review – does your provider have a methodology for continually checking, supervising, and observing risk status to identify changes from the pre-determined performance level? Is there a mechanism to detect changes in context, the risk criteria or risk itself and respond accordingly? And, does your provider have an established auditing process and a solid way to handle compliance concerns?



It's important to note that risk management, particularly in the cloud, is never a once-and-done process. Business continually changes, as does the environment around it. A vigilant service provider has to constantly stay aware of what's going on, recognize and manage the risks, and adapt to the changes.

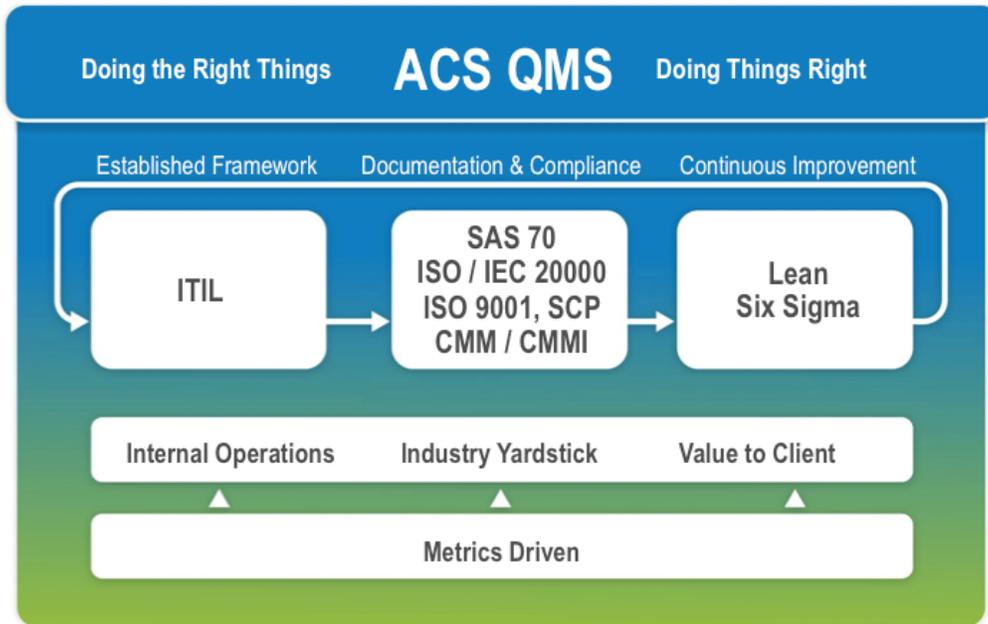


Figure: ACS Quality Management Services (QMS)

For ACS, the standardized, documented, repeatable processes are also critical. The packaging of Lean Six Sigma, ITIL v3, and other tools provide a consistent, repeatable process to drive performance, compliance and continuously align and realign the solution to changing business needs. These comprehensive, documented best practices for ITO services management are essential for effective cloud migration and management to ensure we use the correct processes, documentation and compliance to meet our clients' requirements year over year.

ACS represents the United States Head of Delegation for the International Organization of Standards Committee for ISO 20000. We are the only outsourcer represented on this committee. Our representation means that we not only embrace these standards, but we are helping to shape future standards. ACS is also a member of the U.S. Technical Advisory Group and is part of the IT Service Management Forum (itSMF) Global Certification Committee.

With the ever-growing complexity of distributed IT environments increasing the challenges for successful service management, ACS delivers best-in-class service management capabilities to our clients through ACS Management Platform(AMP), ACS' enterprise-wide strategic initiative to provide a truly integrated IT service management platform. We use AMP to measure and share quality through KPIs, our Balance Scorecard and our web portal.

This platform consolidates service delivery so that our clients can benefit from standardization, an ITIL v3.0 capable solution, and advanced service management capabilities such as Business Service Management (BSM), automation capabilities, and process integration automation.

To be successful, none of this can happen in a vacuum. Trust is built on transparency, which means that, although users may provision cloud in an online self-serve process, in a cloud world, human interaction between provider and client should actually increase. Reporting, continual risk assessment and honest discussions work to ease the fear of the unknown, and continue to build trust in the relationship and confidence in the technology itself. The more virtualized the solution becomes, the more personal the relationship between ACS and client has to become to make this model work.

Choosing the Right Partner for Your Cloud Transition

When IT outsourcing began to radiate the market, companies saw the benefits, but many feared a loss of control, confidentiality and system availability. Although contracts guaranteed service levels, choosing an ITO partner with standardized processes, proven service delivery methodologies, and transparent governance did more to alleviate the fears and move adoption forward than any legal document could alone.

Today, cloud computing is the natural evolution of the ITO model, moving clients from physical data center to a highly scalable, responsive virtual world. So, it follows that those providers that have succeeded in ITO, not only in terms of technology, but open communication, integrity and responsiveness to clients, would be those best positioned to carry interested clients through to a successful cloud deployment.

Look at the history, talk to existing clients, ensure the company has a written process in place for managing the environment, risk and process – then look to corporate stability. Finally, seek out a partner who will put you first with a reputation for doing the right thing – not just in meetings – but every day, in every situation. In short, a company you can trust.

The ACS Experience

At ACS, we recognize the opportunities that cloud brings to the IT marketplace, as well as the fears that may be holding companies back. But, we have the standards and processes in place to help you take the next step. Our track record tells the story.

ACS has been a trusted partner of commercial companies as well as federal, state and local governments. We've successfully delivered critical security services to various federal agencies, including the Department of Homeland Security, the Department of Labor, the Department of Education, and the Department of the Treasury, to name a few. ACS' understanding of the industry security standards, both commercial and federal government, and industry best practices, has enabled us not only to achieve tremendous results in the field of information assurance and security, but also has inspired us to think beyond the 'best practice.'

ACS has achieved maturity in providing enterprise security and security in shared services while offering data center-centric IT services to our clients. By the same token, we believe that a highly trusted cloud security model must be made available by those evolving from a traditional ITO model to cloud model.

One key principal is the cloud security model must be developed using a collaborative approach in which we engage clients in the development of risk management framework and implementation of management, technical, and operational security controls of the cloud. At the same time, we keep our security policy and procedures under a microscope for quick adaptation. Experience is what made ACS well-versed in how federal security is to be handled in a traditional computing environment, therefore, ACS is in a better position to see how security needs be tailored

from agency to agency in the cloud -- as each agency's security requirements cannot be served using an umbrella approach.

When it comes to outsourcing IT services and cloud computing, ACS ensures our customers are in their comfort zone and in control of their information. This approach further builds trust in the cloud. We also work with them to answer these key questions:

- Should the agency or company just dive into the cloud with built-in security?
- What is the best way to evaluate its security offerings?
- How will a client know who is in control?
- How can that client strike a balance between security and business functionalities to be placed in the cloud?
- Last but not least, how does a client establish a cloud resource model?

Answering these questions helps ACS to achieve two key goals for our customers: it sets the transparency in what we have to offer versus what our customer gains, and secondly, it paves a path for key Office of Management and Budget imperatives, such as Federal Information Security Management Act (FISMA) compliance, Health Insurance Portability and Accountability Act (HIPAA) compliance, among others.

Who Do You Trust?

Trust is earned through behaviors, actions, and regimens, which are proven as reliable and accountable. It's something that goes far beyond the terms of a contract or the language in a regulation. As companies and government entities look to cloud as a viable ITO solution, they must first look to a vendor they trust to take them through the process.

For more than two decades, ACS has helped to shape an industry, bringing new efficiencies and cost benefits to our clients. We are positioned to help companies safely take advantage of cloud today, tomorrow and to evolve with the next delivery model in the years to come.

It's the people behind the cloud that makes all the difference.

About the Authors

Chris Mankle is an ACS Chief Technology Officer for the IT Outsourcing business. He is focused on driving and delivering innovation, developing and executing a strategy, recommending the best solutions, creating a vision, promoting innovative solutions, and identifying & driving new business opportunities.

Mars Mariano is an ACS VP Business Development working with government and commercial clients and partners to develop, implement, and advance transformation agile mission business solutions

Mohammad Hasan is an ACS Sr. Information Security Analyst responsible for designing enterprise-level security solutions and providing guidance for the development, enhancement and deployment of large-scale major government systems supporting over 10 million customers. Responsible for policy and directives interpretation (Federal Government) in order to implement proper management, operational, and technical IT security controls all across the federal programs.