Despite a grand entrance into the technology arena, cloud computing has become a point of contention in some organizations. While some department leaders have bypassed their trusted IT departments completely and procured services directly from cloud providers to address immediate needs – claiming reduced costs, faster time to market and improved user experience – some CIOs are not convinced. So how does a CIO survive and remain relevant within the organization if the cloud is viewed as a threat to their existence? Embrace the cloud and evolve your value proposition.
Cloud computing entered the technology arena with great fanfare and promise, presenting a paradigm shift in how technology would be offered – and consumed – and promised to demystify what IT departments across the globe actually do in their “top secret” data centers to make today’s companies run with such intelligence and agility.

Although technology providers have remained fully committed to investing in cloud capabilities, with many changing their entire business model to expand their cloud solutions and capabilities, many Chief Information Officers (CIOs) are still not convinced and are waiting for the buzz to pass. But several years into the paradigm shift, the topic remains very much alive and has become even more relevant, not only for Chief Information Officers but also for Chief Financial Officers, Chief Marketing Officers and many Chief Executive Officers as they struggle to align the ever-so-growing appetite for technology in the modern enterprise with all the complicated technology costs and processes that continue to grow year on year.

In many organizations it has almost become a weapon of sorts, with CFOs threatening IT budgets with the cloud and CIOs aggressively combating the claims of their own trusted providers with arguments of unique capabilities and protection that can only be provided by their internal experts.

The cloud discussion in many organizations starts as a financial opportunity to drive efficiency into technology spend that is immensely complicated and never fully understood by anyone but the CIO. System licensing models, capacity planning forecasts, software support contracts, business continuity configurations and non-production landscapes are lively conversations when explaining the total cost of ownership to a department leader sponsoring a new business initiative. In contrast, the cloud offerings seem almost too simple. You determine what you need, for how many users and the method of payment. At times it can really be that simple but in most cases there are additional items to consider and should be fully evaluated in advance of any commitment. What is a technology leader to do when their CMO requests a global media streaming solution to allow real-time presentations, knowledge sharing and improved corporate training within six months and presents the request with board approval and funding? This will require new skills, new technology and possibly a revamp of the entire infrastructure. However, the budget approved only covers a fraction of what is needed and was based on marketing material from a cloud provider and monthly pricing presented on the provider’s website. For technology leaders they will not know where to start.

In many companies it may not quite happen this way but for many this is how expectations are first set. As the CIO, do you admit defeat and walk away? Let the CMO bring in their preferred vendor and remove yourself from the conversation?

Never. If anything, the CIO should wear the internal hat of cloud expert, never the anti-cloud lobbyist. Become well versed in what the market offerings are proposing.
and how. Understand how they can be leveraged within your company, the pitfalls as well as the hidden costs and considerations. Update your enterprise architecture and strategy to consider cloud technologies and how they will fit into the broader landscape for business intelligence, reporting and data protection. In some cases, selecting a cloud offering is the only feasible solution. Prepare for this in advance. Be the first person engaged when a cloud idea arises, put in place the necessary controls and capabilities that will prevent the cloud from disrupting what is already in place and working today and champion the change across the organization.

As the CIO, do you admit defeat and walk away? Let the CMO bring in their preferred vendor and remove yourself from the conversation? Never. If anything, the CIO should wear the internal hat of cloud expert, never the anti-cloud lobbyist.

Many technology leaders spend endless hours ensuring that all systems are built to last and performing as expected. Systems are up and running, sufficient capacity is on hand, operating procedures are in place, all while keeping a close eye on variable costs. In the cloud-enabled world you may not be as involved in the daily details of operating such technical elements. However, someone has to be aware of what is happening every day. Are services meeting the contracted levels of performance and stability? Are business and user expectations being met? As the CIO and custodian of all things technology, embrace this opportunity to become the broker between your business and cloud providers. You may not own the assets nor have visibility in how they are operated but you do have the responsibility of ensuring the business is realizing the value of their investment. Put in place strategic vendor management disciplines that consistently measure the cloud provider’s performance with effective controls that drive accountability. Benchmark their performance and capabilities against competitors and ensure that the needs of your business are clearly understood and delivered upon. This may feel closer to a procurement officer role but as the trusted technology expert, the CIO is best positioned to interface with cloud providers and manage the commercial relationship on behalf of their business.

Do not compromise on expectations and results because the service is being managed externally.

What happens if the cloud turns to rain?
The greatest fear and hold off for most organizations adopting cloud services is the loss of control. Mature providers have responded well to this concern and offer very comprehensive and stringent agreements that cover the best interest of any organization with the appropriate recoveries, penalties and warranties. But what do you do when disaster strikes? Do not wait for the unforeseen, be proactive.

• Governance and controls - Alongside the effort to update the enterprise architecture and strategy, revisit governance processes, security standards and compliance programs to ensure that cloud-based services are considered and provisioned for. Put in place specific standards that must be complied with for all cloud-based services, detail requirements that must be met to uphold security posture and be explicit on what must be considered prior to committing to any service. This should not evolve into a situation in which cloud services will never qualify, but rather a guideline of how to proceed and what to watch out for. If anything, this should simplify the review and selection process.
• End users - The ever-growing popularity of BYOD (Bring your own device) and mobility solutions has introduced many consumer-focused solutions that are leaking into the enterprise. It is very challenging to stay ahead of all the solutions and services that are being downloaded by users every day. An easier approach to adopt is one of education and policy. Help users understand how to protect themselves and their employer in the digital world. Define usage policies that clearly articulate how information should be handled, shared and protected. Make it simple but make it clear.

• Business continuity and exit - Establish a plan for the worst-case scenario. Implement an exit strategy that ensures that you have access to your information and the ability to recover from a technical or relationship crisis. Understand the impact and planned reaction in the event of a major failure and test this. Test the security, privacy controls and procedures of the cloud provider to understand the potential for exposure or breach. As the guardian and protector of all digital assets, ensure that data hosted outside of your control is included in your risk management reviews, security assessments and planning.

The cloud has come a long way and will continue to evolve in capability and relevance. It will force change within organizations and disrupt business-as-usual for IT departments across the globe. However, the cloud will not replace enterprise IT departments. To fully realize the potential, prepare your organization and yourself to capitalize on this window of opportunity. Lead the change through proactive planning, embrace the change through increased knowledge and participation and embed the cloud within your IT strategy with effective standards, controls and measurements.

As the trusted technology expert, the CIO is best positioned to interface with cloud providers and manage the commercial relationship on behalf of their business. Do not compromise on expectations and results because the service is being managed externally.

by Basit Saeed, Chief Information Officer, IT, Deloitte Middle East