MOBILE

Executive Insights for Building Trust in the Cloud

BY ITBE STAFF FEBRUARY 19, 2014

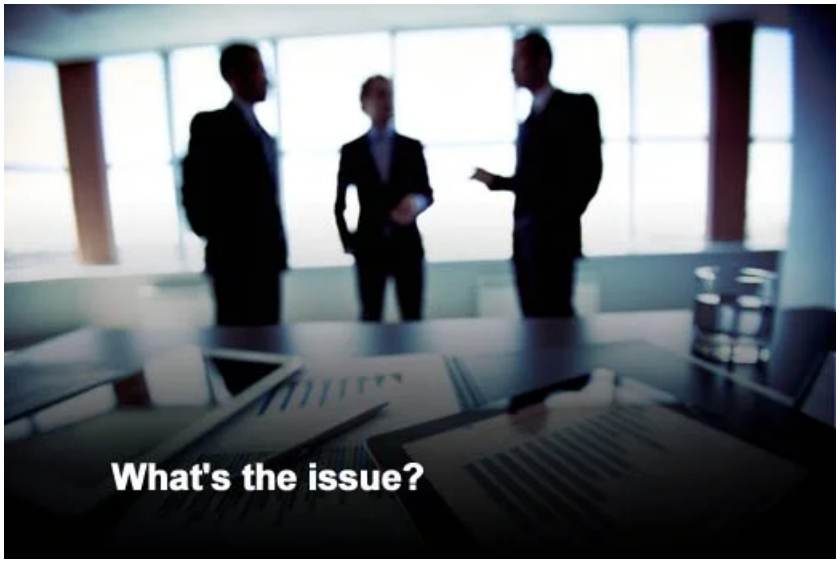
Not that long ago, cloud computing was little more than a speck on the horizon. We heard reports of it rapidly becoming a mainstream technology, but it had yet to make a meaningful impact on our technology landscape. According to EY's Global Information Security Survey, in 2010, 30 percent of respondents indicated that their organization used or was planning to use cloud computing-based services. In 2011, the percentage had risen to 44 percent. By 2012, cloud computing had reached a technological tipping point: Almost 60 percent of survey respondents said their organization was using or planned to use cloud computing services. And yet, 38 percent of respondents said that they had not taken any measures to mitigate the risks of using cloud computing services. This disruptive technology was advancing faster than many could secure it.

A more recent Forrester Research report suggests that for 73 percent of surveyed businesses in Europe and North America, security remains a major concern when considering cloud computing.

One of the first principles of improving information security is taking control of your environment. It would therefore feel counterintuitive for an organization to surrender control of its IT infrastructure and data to a third party. And yet this approach may offer the best opportunity to address increasingly complex security and privacy challenges. Rather than becoming an organization's worst security nightmare, cloud computing platforms may offer its best hope to create a more secure IT environment by strengthening controls and improving information and security capabilities.

Here are five insights for executives from EY for creating an environment that is secure, trusted and audit-ready.

Click through for insights for executives from EY for creating a cloud environment that is secure, trusted and audit-ready.



What's the issue?

No longer considered an emerging technology, cloud computing services have entered the mainstream. Today, a significant majority of organizations have either adopted or are planning to adopt some form of cloud computing technology. Whether CIOs know it or not, their data and corporate boundaries have entered the cloud. Business units, departments and business partners are engaging directly with cloud services providers without first consulting IT: a phenomenon EY calls "cloud creep." The lines of our once clear corporate network boundaries are now blurry.

Some fear that communicating data over a public network will increase its vulnerability to cyber attacks. Others worry that cloud service providers offering the same infrastructure to multiple clients in multiple locations will not be able to maintain segregated confidentiality. Still others express concern that transmitting their data across international boundaries will expose them to diverse legal and regulatory requirements in jurisdictions with which they're unfamiliar.

What's the issue? continued

Unfortunately, these fears and IT's perceived need to retain physical controls over its environment can increase an organization's risk rather than mitigating it. Within many organizations, when business units that want to use cloud computing hear "no" from IT, they simply go off and procure the service themselves. This not only extends the organization's IT environment without the right protections in place, but it also takes cloud computing into the shadows where IT can neither anticipate nor address the resulting risks.

IT must shift its focus from saying "no" to saying "yes" in a way that adds value to the business and protects it from mounting cybersecurity risks. Developing a cloud framework that creates a secure, trusted and audit-ready (STAR) environment may be just what IT executives need to say "yes" with confidence.

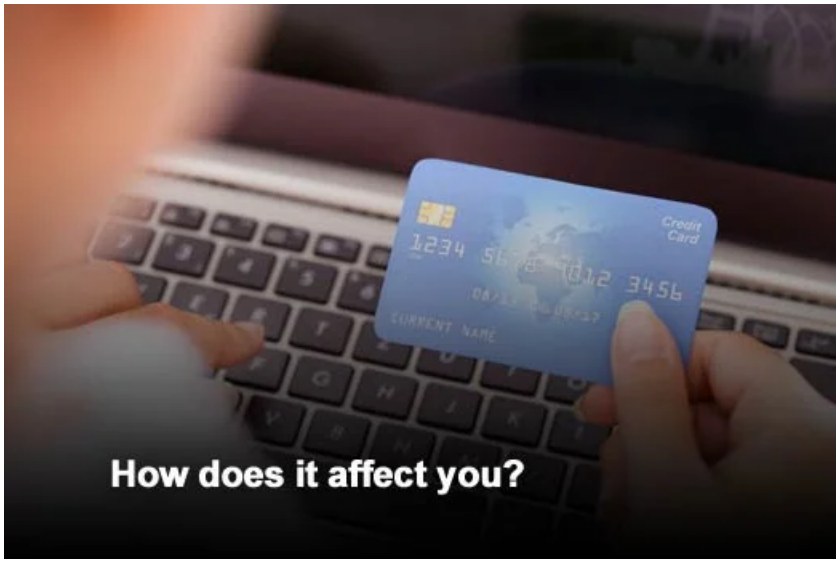
Why now?

Whether IT professionals like it or not, cloud computing services have become an integral part of day-to-day business activities. Between 2010 and 2012, cloud adoption rates nearly doubled. Those who have embraced cloud-based services have generated internal efficiencies,

attracted new customers, discovered new avenues to market their products, increased internal collaboration and gained an overall advantage over their competitors.

IT executives who have not worked with the business to embrace the cloud have seen a marked increase in shadow IT within their organization and a corresponding decrease in their influence within the organization. In EY's 2013 Global Information Security Survey, only 17 percent of participants indicate that their information security function fully meets the needs of the business. Changing information security's mindset to help the business find a path rather than block it is the challenge that organizations face.

Cloud-based services are here to stay. IT functions need to learn to either work with them or suffer the cybersecurity and financial consequences that may result in having cloud adoption take place without the input and value of IT.



How does it affect you?

It takes little more than 15 minutes and a credit card to purchase and set up a cloud solution, making it an easy workaround for business executives that too often hear "no" from their IT

functions. In large organizations, the proliferation of this phenomenon without IT oversight creates growing security, privacy and financial risks to the organization.

Even those organizations that have adopted cloud services are exposed. Often, there is a gap between the controls typically implemented in the cloud and the controls necessary to create a secure, trusted and audit-ready cloud environment.

What's the fix?

Since banning cloud services within an organization is not an option, IT executives should shift their focus toward building a secure, trusted and audit-ready (STAR) cloud environment.

Secure

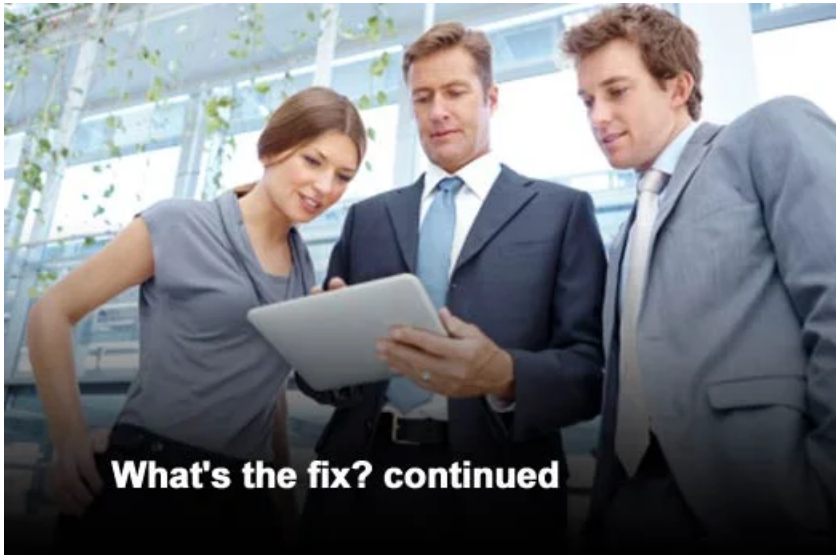
A secure cloud environment has the appropriate controls to protect the confidentiality, availability and integrity of the systems and data that reside in the cloud. Appropriate procedural and technical protections are in place to protect data at rest, in transit and in use.

Trusted

A trusted cloud environment is designed to stand the test of time. It should provide high availability and resilience to adverse events.

Audit-ready

An audit-ready cloud environment has continuous compliance and is certified to meet specific industry regulations and legislation. Appropriate procedural and technical protection is in place, documented and can be verified for compliance purposes.



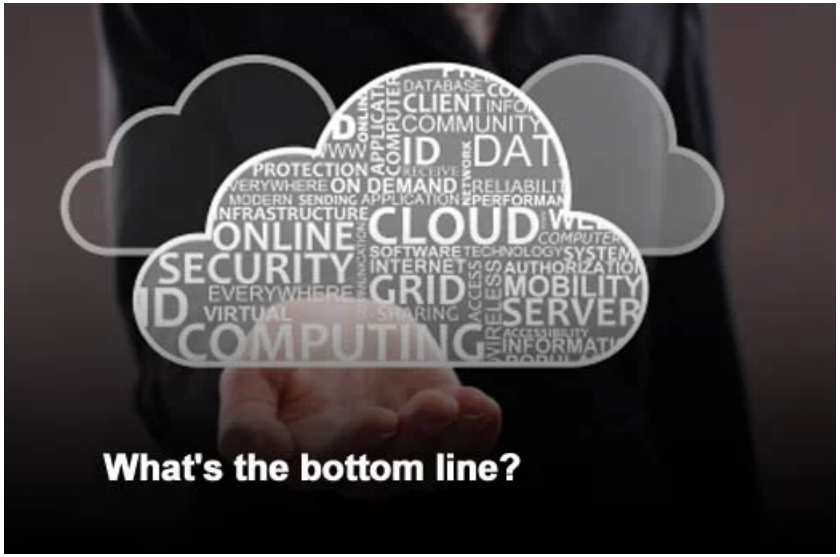
What's the fix? continued

These six domains contain the various controls and procedures required to support a STAR environment. This model can be flexible and should accommodate the different cloud deployment models so that IT can provide clear guidance to the organization to promote responsible adoption of the cloud.

- **Organization.** Cloud services impact the organizational behaviors. Organizations need to document roles and responsibilities associated with the use of cloud services and train employees regularly on these protocols.
- **Technology.** IT functions should design applications according to industry security standards, encrypt the data, and implement role-based access and identity management solutions.
- **Data.** IT functions need to classify and inventory data, assign data owners and securely purge data that is no longer required.
- **Operations.** Business continuity management (BCM) and resiliency program policies and procedures should include periodic review and testing. Additionally, policies and procedures for BCM, change management and data center security should be documented to formalize roles and responsibilities.
- **Audit and compliance.** Organizations should plan and execute audits in a way that minimizes business interruption. For maximum assurance, organizations should engage a third party to perform the audit and certify the environment.
- **Governance.** There are many cloud options from which organizations may choose, from public cloud services, to building a private cloud, to a hybrid approach. Regardless of the deployment path organizations pursue, governance processes should be scalable, repeatable, measurable, defensible and constantly improving.

Using the model as a foundation, IT functions can then create a framework to:

- Assess and monitor by evaluating the organization's current risk profile and then developing a plan to address key areas of exposure.
- Improve and enhance by executing remediation activities that support the plan.
- Certify and comply by obtaining third-party assurance that the organization's cloud environment is secure, trusted and audit-ready.



What's the bottom line?

Widespread consumption of cloud services isn't on its way. It's here. Early adopters of cloud services have already gained competitive advantages. It is clear that those organizations who can think "cloud first" while managing their risks through a clear cloud trust model are benefiting from the efficiencies, cost savings and additional capabilities that cloud brings.

By creating a framework based on six cloud control domains, organizations — regardless of what stage they are at in their cloud journey — can create a cloud services environment that is secure, trusted and audit-ready. The key is to find ways to balance the real and perceived risks with the value of adopting a cloud solution that improves the security of an organization's intellectual property.