Sponsored by: **Microsoft**

Authors:
Sean Pike

June 2017

The Rise of the Cloud Compliance Professional

Understanding this Critical Role in Digital Initiatives

OVERVIEW

Cloud technologies are the fuel for digital transformation initiatives and operational efficiencies. As such, the way cloud technologies are used to disseminate information is facing unprecedented scrutiny and regulations. While regulation may hinder innovation for the average enterprise, a more significant risk may be the unrestrained adoption of the cloud itself. Consider the prevalent use cases for cloud: lines of business (LOBs) use cloud to develop products and back-office functions seek to streamline operations. New uncertainty surrounding cloud adoption threatens an organization's ability to effectively leverage the cloud. Should uncertainty prevail, many of the cloud's benefits — including digital transformation initiatives — will go unrealized. Yet uncertainty around the cloud exists, in part because of highly anticipated, far reaching regulatory efforts like the General Data Protection Regulation (GDPR) which could broadly increase regulatory risk.

If IT executives feel disconnected or blind to the inner workings of cloud or cloud-specific security architectures, this too will contribute to uncertainty. This lack of visibility further increases anxiety surrounding regulation and enterprise-specific requirements. Finally, those IT professionals who are typically charged with architecting or securing efficient IT solutions often do not have the proper training. These individuals are not equipped to adequately deal with both the technical aspects of the cloud and the cloud's potential legal ramifications. Regardless of the specific reason for uncertainty, cloud adoption is at a critical juncture. The benefits of the cloud in terms of cost, scale and speed are far too great to ignore. Organizations realize this, judging by the rate at which they have moved traditional on-premise functions to cloud-based architectures. In addition, many organizations are now taking a "cloud first" approach when developing new initiatives.

"We embrace cloud because it gives you flexibility and scalability… but we approach cloud cautiously for sensitive data. From that perspective, we must ensure [cloud providers] meet necessary regulatory and security standards."

IT Decision Maker/ Large Transportation Industry Company

"We embrace cloud because it gives you flexibility and scalability… but we approach cloud cautiously for sensitive data. From that perspective, we must ensure [cloud providers] meet necessary regulatory and security standards."

—IT Decision Maker/Large Transportation Industry Company

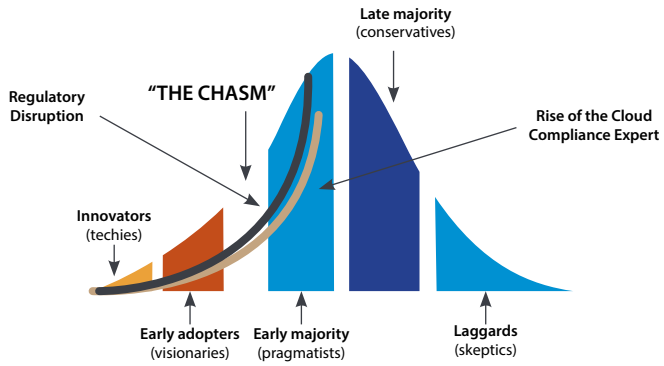
IDC
Analyze the Future

Cloud adoption has long since "crossed the chasm" in terms of innovation and adoption. A recent IDC survey reveals that 80% of respondents already deploy cloud-based architecture. Looming regulation aimed specifically at cloud or cloud-supported functions however, threatens to interrupt this momentum by introducing layers of uncertainty. Regulation typically trails behind standard technology adoption cycles. When technology is adopted by a relative minority, it is not pervasive enough to propel slow moving regulatory bodies to act. As technology adoption increases, regulators take notice. This is especially true in situations where new technologies modify how consumers and businesses interact with previously regulated data or delivery mechanisms. Cloud architecture accelerates the development of new technologies and creates worldwide data accessibility; it was only a matter of time before regulators respond. Today, emerging regulation is focused on reining in the perceived security and risk challenges cloud architecture presents. Thus, enterprise cloud champions must adjust their adoption strategies by including complementary regulatory and risk management expertise.

Enterprise cloud planning now requires detailed and sometimes painful discussions about the regulatory and legal risks associated with any new cloud initiative. Champions can no longer focus solely on the cost/time equation that fueled cloud adoption rates in the past. Such traditional cloud economics ignore compliance and risk considerations. Now, cloud initiatives require an in depth understanding of regulatory mandates, internal policies, legal exposure, business strategy and more. Cloud adoption and the digital transformation initiatives that have followed have already strengthened the relationships among IT, IT security, and LOB professionals. The growing need for additional risk and compliance expertise is strengthening the relationships between IT stakeholders and their key counterparts within the legal, risk and compliance departments. From this collaborative union, a new breed of cloud compliance expert has emerged — an individual with specific legal knowledge, compliance skills and technical competencies who helps further bridge traditional disconnects between IT, IT security, and risk management (see Figure 1).

FIGURE 1

Rise of the Cloud Compliance Expert



Source: Crossing the Chasm, Moore, G. 1991

"We have a limited number of [cloud] providers that we are going to go with so they are strongly vetted."

IT Decision Maker/Large Healthcare Industry Company

The Importance of Trust

Strengthening relationships, however, is only the beginning of cloud compliance efforts. Together, all parties must strive to find new and appropriate ways to adopt cloud pursuant to business risk, tolerance and regulation. Identifying internal needs and performing external capability assessments to identify vendors capable of delivering specific requirements is essential, and in this scenario trust becomes paramount.

"We have a limited number of [cloud] providers that we are going to go with so they are strongly vetted."
—IT Decision Maker/Large Healthcare Industry Company

After vendor selection is complete, internal stakeholders realize they must eventually cede control to a selected cloud platform partner, placing trust firmly in both the selection process and the providers themselves. This begs the question: "What is trust?"

Along with Microsoft, IDC developed a profile for trusted cloud by defining six key selection criteria: security, privacy, control, transparency, compliance, and reliability. Survey respondents told IDC that the combination of such criteria outweighs cost and feature/function metrics when selecting a cloud platform.

In This White Paper

This IDC white paper explores the emerging role of the cloud compliance profession and how this role intersects with professionals in the legal, compliance and technology departments. This paper further discusses the regulatory issues created by disruptive new technologies — specifically as regulations relate to cloud adoption. In addition, the paper will examine how trust plays a role in cloud platform selection, digital transformation initiatives and ultimately the relationship between an organization and its cloud platform provider.

Survey results referenced in this paper are from a global web survey of 1,091 enterprises conducted in 2016 in Argentina, Australia, Brazil, Colombia, Germany, Hong Kong, India, Indonesia, Japan, Korea, Malaysia, Mexico, Russia, Singapore, the United Kingdom, and the United States. Survey respondents were cloud compliance professionals with power to veto or delay cloud deals on compliance grounds. Organizations ranged in size from 500 employees to over 50,000 employees and spanned numerous diverse industries.

IDC Perspective

IDC believes that cloud architectures and cloud compliance professionals are an integral part of business success. Cloud architectures provide businesses with the opportunity to stretch IT budgets by avoiding capital expense while speeding time-to-value and reducing the burden of hardware maintenance. This has made cloud the strongly preferred first option for new initiatives and technology refresh projects. Recently in efforts to protect the rights of its citizenry and prevent fraud, regulatory bodies have targeted the unfettered exchange of data. As an enabling technology, this places cloud squarely in the crosshairs of new regulations.

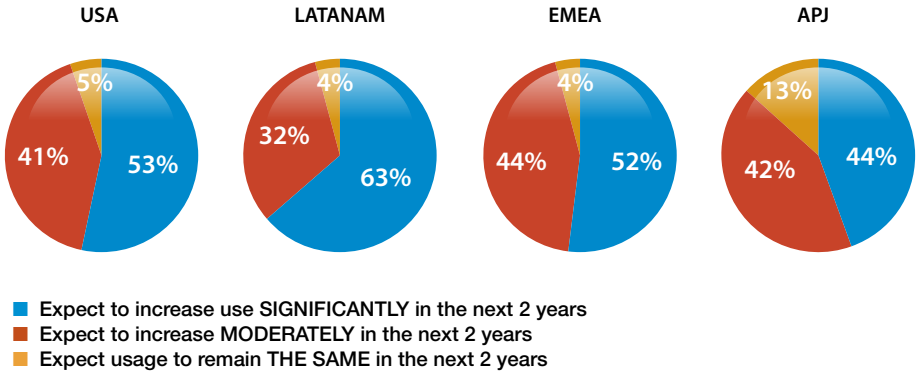
Cloud compliance professionals help enterprises navigate new regulatory demands to ensure corporate compliance. These individuals have a unique set of skills which can help LOBs push forward through digital transformation initiatives while identifying and avoiding risk. Due to the pervasiveness of cloud adoption and expected growth, the stature of these professionals will only increase in the future as they become integral participants in the transformation process. Ultimately, these individuals will have significant influence over technology and cloud provider selection.

Cloud Beyond the Chasm

Cloud adoption is already pervasive. IDC's most recent Public Cloud Services Spending Forecast shows that worldwide spending on public cloud services will reach $122.5 billion in 2017 which represents an increase of 24.4% over 2016 spending. Further, IDC expects a five-year compound annual growth rate (CAGR) of 21.5%, nearly seven times the rate of IT spending overall. More recently, an IDC global survey of mid-size and large enterprises showed that nearly 80% of the respondents already employ cloud services, whether cloud infrastructure (IaaS or PaaS) or applications (SaaS). Of the respondents that already leverage cloud, nearly 95% expect some level of increase over the next two years, and over 50% expect significant increase over the next two years (see Figure 2).

FIGURE 2

Cloud Adoption by Region



Source: Microsoft Cloud Compliance Survey, 2016
n=1,091; USA-EMEA-LATAM-APJ

Adoption Drives Regulation

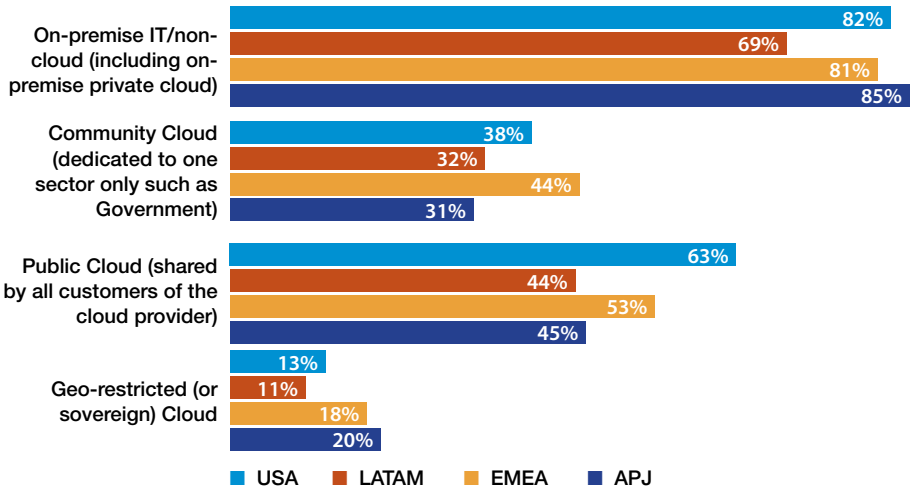
These statistics are overwhelming. Cloud technologies have "crossed the chasm" presented by more recent Diffusion of Innovation theories. In effect, technology adoption is not entirely a one-way conversation. Any number of external factors guide adoption. To achieve maximum adoption, the innovation itself must be modified and presented in ways that meet the needs of all levels of adopters. This process is characterized by five categories of adopters: innovators, early adopters, early majority, late majority, and laggards. As adoption over time proves beneficial, innovation spreads to a critical mass.

Based on the survey, it is clear that cloud technologies have indeed crossed the chasm. In fact, a direct map to Rogers' Diffusion of Innovations curve would show that public cloud services have reached the top of the Late Majority category. In the same survey, geo-restricted (sovereign) and community cloud (dedicated to a specific vertical) are trailing behind in adoption but have also generally gone beyond the chasm. The narrow exception being geo-restricted cloud in the United States. The longer adoption tail for geo-restricted cloud and community cloud is apropos.

FIGURE 3

Cloud Types in Use

Q. Which of the following types of cloud and non-cloud application or platforms is your organization currently using?



Source: Microsoft Cloud Compliance Survey, IDC, September, 2016
n=1,091; USA-EMEA-LATAM-APJ

The Regulatory Tail

Regulation often comes on the heels of innovation. That is not to say that regulation always follows innovation but, when it does, it must be applied after adoption of the initial innovation and likely after innovation has crossed Moore's chasm. It is generally accepted that regulation comes sometime after widespread adoption — something commonly referred to as the regulatory tail. When technology only exists in the hands of a small portion of the population (15% before the chasm), there is little need to contemplate regulation. However, as technology adoption rises to include a larger segment of the population, regulation becomes necessary. Essentially, regulation that targets the unfettered movement of data forces highly regulated industries to adopt solutions with built-in control mechanisms. This is where the cloud compliance professional comes in.

Regulatory Innovation

In mature, regulation-heavy countries, federal data protection regulations or guidelines have existed for some time yet none have sufficiently addressed the cloud phenomenon. In Germany, the implementation of the first federal data protection act occurred in 1979. The Organization for Economic Co-operation and Development (OECD) — a 35 country

economic development consortium — first published its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980. These guidelines later helped to shape Data Protection Directive 95/46/EC — an attempt to harmonize data protection regulations across the EU. In the United States, lawmakers have traditionally taken a fragmented approach to data protection targeting regulations to specific industry challenges. The Federal Trade Commission Act (FTC Act), for instance, has broadly allowed the Federal Trade Commission (FTC) to pursue privacy and data protection cases on behalf of consumers. The Health Insurance Portability and Accountability Act (HIPAA) and the Graham-Leach-Bliley Act (GLBA) provide for data protection within the healthcare and financial services sectors respectively. None of the existing data protection regulations fully contemplated "cloud" and all the implications widespread adoption would bring.

Where no specific regulation exists, courts are forced to apply existing laws to new challenges. In some cases, this means applying physical laws to digital problems or laws targeted at specific technologies to altogether different technologies, creating a lag between technology and targeted regulation. This phenomenon gives us the current state of cloud regulation. Data protection regulations exist but it has traditionally been difficult to apply existing regulations to the speed and scale that characterize cloud implementations. This is one of the reasons that the GDPR is so important as it begins to contemplate the scale of cloud and new data sharing economies that result. While the GDPR is targeted to protect EU citizen data, it implicates any company that may be defined as a data processor or data controller as it relates to EU citizen data no matter where in the world that company is located. For many companies, the repercussions of GDPR's scope is disconcerting. Consider the following under GDPR:

- Fines may be up to 4% of global revenues
- There is a 72-hour breach notification requirement
- Joint liability may exist between data controllers and processors
- Any data that identifies an individual is personal data
- Individuals have the right to access their data and have it deleted

This regulatory effort follows growth of digital transformation initiatives. Companies are thinking more about global reach and the cloud helps accelerate that process. Regulators will continue to follow suit and it is highly likely that additional regulatory efforts will be needed as cloud adoption and digital sharing economies expand and evolve.

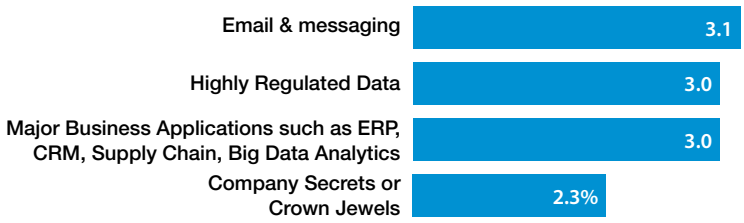
While it may be obvious that security and compliance are highly connected, it is important to note that regulations affecting cloud initiatives may not always give core security principles — confidentiality, integrity and availability — the same weight. GDPR, for example, has a strong component of data protection aimed at preserving privacy or confidentiality. It also has some provisions related to integrity and availability, especially in terms of Right to be Forgotten requests. However, GDPR is widely seen as a privacy or confidentiality regulation.

The distinction between security and compliance is important. Security has long been a cloud consideration. In fact, there is a long-standing tradition of avoiding cloud security risk by choosing to keep certain workloads on-premise because these workloads were deemed too important or too sensitive. To a degree, that bias still exists. Figure 4 shows the comfort IT executives have with public cloud in relation to workloads with varying degrees of sensitivity. What is important to remember, however, is that security and compliance are not wholly synonymous.

FIGURE 4

Public Cloud Trust by Application

Q. Indicate the degree to which you trust public cloud infrastructure for each IT application or data. (1 = very low trust and 5 = very high trust)



Source: Microsoft Cloud Compliance Survey, IDC, September 2016
n=1,091; USA-EMEA-LATAM-APJ

A New Ecosystem

As a natural result of increased technology-focused regulation and litigation, individuals skilled in law, risk/compliance, or the technologies themselves are challenged to adapt to new requirements and participate in the technology decision-making process. Over time, this evolution can create disruption in the adoption of specific technologies.

Regulations and court opinions that shape how regulation is established and applied are not typically black and white. Often, individuals must interpret whether enterprise activities fit within the meaning of regulations. Even then, interpretations come with a level of risk. As technology-specific regulation grows, so too does the practice of interpreting the regulation and assessing associated risk.

Thus, today's compliance and legal professionals are much more integrated into the enterprise technology adoption process than ever before. Cloud is the next evolution of this involvement for these professionals. In-house legal and compliance staff are quickly becoming adept in the language of cloud; these professionals are brought into the cloud selection process as cloud compliance experts and decision makers. The presence of these professionals in this process challenges existing IT decision-making practices.

IT decisions were once the exclusive domain of IT personnel. Over time, LOB managers became more involved in IT decision making. With the cloud, LOBs soon took on sole ownership of many IT decisions by provisioning systems and services on their own. The last few years — as data security has become a top concern — have necessitated more collaboration between IT and LOBs. The goal is for these groups to build sustainable, scalable architecture that provides better enterprise visibility into IT spend while also pursuing digital transformation.

Cloud architecture is a major driver of this collaboration as LOBs are typically unable to sustain prolonged shadow IT initiatives and IT can help control costs through enterprise-wide transformation efforts. While LOBs and IT professionals need to ensure new technologies meet business needs and are technically feasible and secure, cloud compliance professionals must ensure that prospective cloud environments do not create undue risk. Since cloud architecture is so closely tied to digital transformation, LOBs, IT, and cloud compliance professionals find themselves working together to develop strategy. And in terms of the cloud provider selection process, compliance professionals appear to wield a certain amount of power.

Cloud Authority

We asked respondents in our survey about the relevance of specific standards when evaluating and selecting a cloud service provider. At least 50% of cloud compliance professionals told us that they pay close attention to almost every standard that may influence the choice of a cloud provider (Figure 5).

FIGURE 5

Importance of Standards

Q. How important are the following regulatory or compliance issues in choosing Cloud Application or Platform providers?

Note: Percentages indicate the number of respondents who cited the issue as important.
Source: Microsoft Cloud Survey Compliance, IDC, September, 2016
n=504, USA–Germany–UK

Considering today's cloud-centric digital transformation strategies, enterprises are placing a tremendous amount of responsibility with the cloud compliance professional. Consequently, these professionals must work closely with IT/IT security and LOBs to identify technology providers of choice. Given the shared responsibility model of a successful cloud implementation, many organizations wonder how best to select a cloud technology partner; in many cases, it comes down to building trust.

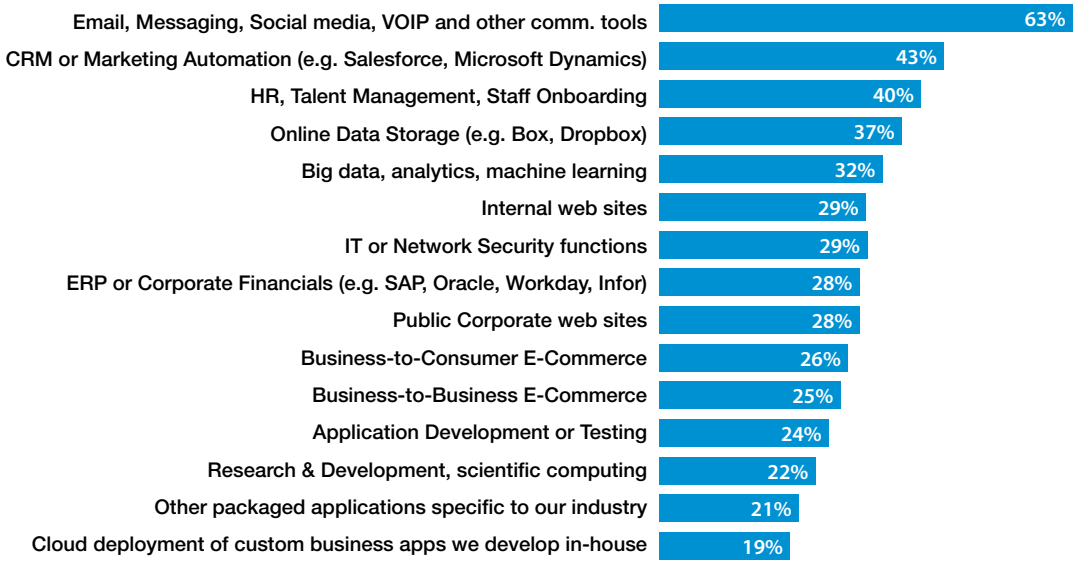
Advancing the Ecosystem (Building Trust)

In addition to the use of different cloud services (e.g., public, community and so forth), organizations have traditionally been reluctant to move to the cloud. Email, messaging, and social media top the list of cloud-supported business functions (see Figure 6). It's worth noting that Microsoft's Office 365 or Google's G Suite have gone a long way toward pushing enterprises to adopt cloud-based productivity platforms, but there also seems to be a general comfort with these types of applications moving to the cloud infrastructure. Perhaps, it's the nature of email that makes the transition easier to bear. Email is meant to be a sharing platform, and if employees are following existing data protection policies, theoretically email won't contain the most sensitive corporate data.

FIGURE 6

Deployed Public Cloud Applications

Q. For which business functions does your organization rely on cloud applications or platforms?



Source: Microsoft Cloud Compliance Survey, IDC, September, 2016
n=1,091; USA-EMEA-LATAM-APJ

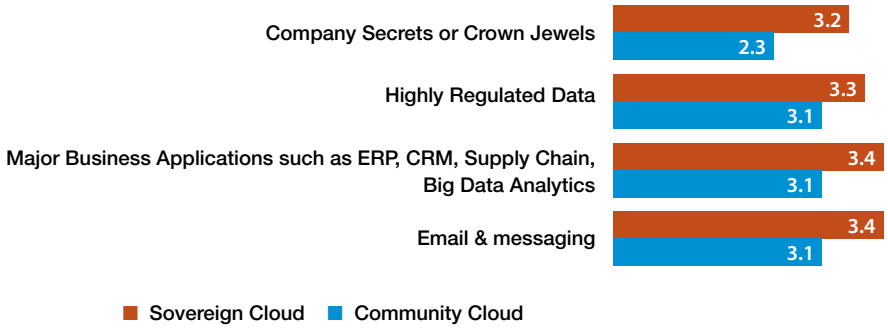
In sharp contrast, only 17% of respondents use cloud infrastructure for ERP and corporate financial systems, which is directly attributable to the nature of the data stored within those systems. Business process and financial data are integral to the inner workings of the business so there is a natural tendency to hold that data closer to our sphere of control. Indeed, IDC research shows that cloud decision makers tend to place more trust in environments where they perceive higher levels of control for sensitive data.

In the case of public cloud, decision makers trust proprietary company data, as well as highly regulated data, primarily to on-premise architecture. Public cloud architecture is trusted for email and messaging more than other types of data (see Figure 7).

FIGURE 7

Community Cloud and Sovereign Cloud Trust by Application

Q. Indicate the degree to which you trust community cloud and sovereign cloud infrastructure for each IT application or data. (1 = very low trust and 5 = very high trust)



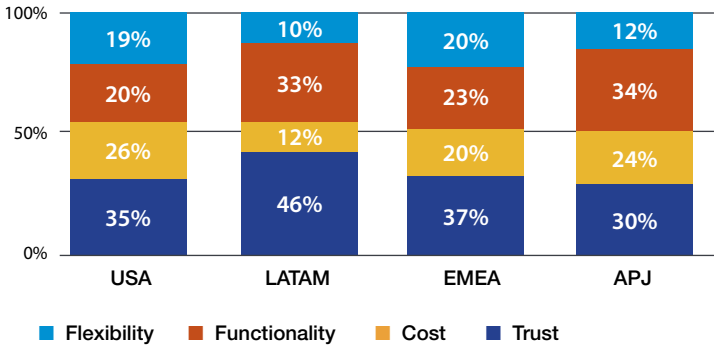
Source: Microsoft Cloud Compliance Survey, IDC, September, 2016
n=1,091; USA-EMEA-LATAM-APJ

How important is trust? According to our survey respondents, trust is the number 1 factor in considering a cloud vendor; functionality trails slightly behind (see Figure 8). The importance of this finding cannot be overstated. Organizations are laser focused on digital transformation, yet functionality ranks behind trust in terms of requirements.

FIGURE 8

Cloud Selection Factors

Q. What is the most important factor in choosing a cloud provider?

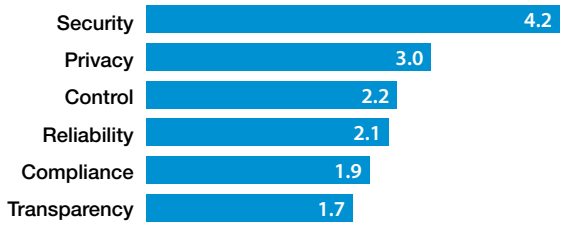


Note: Current cloud users
Source: Microsoft Cloud Compliance Survey, IDC, September, 2016
n=1,091; USA-EMEA-LATAM-APJ

FIGURE 9

High Priority Trust Factors When Evaluating Cloud

Q. Thinking about these 6 trust factors, please rank the relative priority your organization assigns to each when evaluating a new cloud application or platform.
(1= least important, 6= most important)



Source: Microsoft Cloud Compliance Survey, IDC, September, 2016
n=1,091; USA-EMEA-LATAM-APJ

Conclusion

The importance of cloud architecture cannot be understated. It is so pervasive that nearly every enterprise is adopting or exploring adoption of cloud to enhance or replace existing enterprise architecture models. Regulation is threatening to derail or at least slow down this trend. When cloud adoption was relatively immature, enterprise adoption required minimal consideration of compliance. Security was certainly considered, yet global regulations are now mandating security mechanisms in addition to those related to availability, performance, and other standards. As a result, a coordinated enterprise effort is required to select technologies which best suit digital transformation initiatives. As part of that effort, a new breed of cloud compliance professional is required to bridge the requirements of regulation among IT and LOB personnel.

Digital transformation is a strategic imperative, one that requires massive use of cloud among other technologies. Since the cloud requires entrusting critical data to partners, creating a well-defined and regulated framework for trust between cloud providers and their customers is essential.

IDC Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Analyze the Future