Microsoft

Think Cloud Compliance

New International Standards Will Help Cloud Customers Understand and Control Risk

Craig Shank,
Vice President,
Corporate Standards,
Microsoft Corporation

Cloud computing offers tremendous economic benefits, but it raises a host of critical challenges for legal and compliance professionals in customer organizations as well as for regulators. Vendor-neutral regulations that set minimum standards for the security and privacy of data transfers between cloud providers and cloud consumers allow the cloud ecosystem to flourish. In this article, I will present and discuss a new international standard that will make it easier for organizations buying cloud computing services to systematically compare what different cloud providers are offering. Before I discuss the role of standards, let me first take a step back and explain the true scale of the cloud computing phenomenon.

> "...in 2013, the number of server applications running in cloud data centers surpassed the total in traditional on-premises data centers."

Looking back now, it was in 2013 that the world of computing changed forever. In that year, the number of individual server applications running in the world's cloud data centers surpassed the total of those running in traditional data centers for the first time. This trend has been accelerating ever since. The present decade will see a complete reversal of roles between on-premises data centers – where businesses and government agencies have traditionally done their computing – and the cloud. From hosting just 21% of all server applications in 2010, the percentage of applications running in the cloud is expected to rise to 86% by 2019[1]. Although on-premises computing will likely never disappear completely, its function will be reduced to running just a tiny fraction of legacy computing workloads.

What is driving the cloud revolution? The answer lies in a confluence of technical innovations and volume economics. Starting in the 1990s, the rise of the Internet made universal connectivity much cheaper compared to older mainframe networks. Today, nearly every potential customer has access to fast, cheap networks. On the data center side, cheap commoditized servers that evolved from PCs lent themselves to far larger concentrations of computing power than ever before. In the mainframe era, data center size was limited by the scale-up nature of mainframes – you can put only so much computing capacity in one box. Today's scale-out architectures have no firm technical limits on how large they can grow – when you can go on adding new racks of servers for as far as the eye can see, it's only a question of investing enough capital to meet customer demand. Another key to the rise of cloud has been the spread of standardized server-side software that offers greater sophistication than the previous era's mainframe software at a far lower cost[2].

> “… only 28% of the cloud agreements are signed with the involvement of corporate counsels.”

The most important consequence of the cloud revolution is that by driving an exponential drop in the cost of computing and network connectivity, it makes possible a continuing flood of new applications that were previously impossible.

However, the accelerating adoption of cloud computing in today’s enterprises has caught many of the stakeholders responsible for corporate compliance and governance unprepared. Corporate counsels, risk managers and procurement departments often find themselves left out of the loop when line of business managers, having discovered that cloud deployments do not require large up-front capital investment, abruptly decide to shift operations to the cloud. A recent Forrester Research study, for example, finds that only 28% of the cloud agreements are signed with the involvement of corporate counsels[3]. When these key stakeholders do participate in the decision, they are often left without a framework to structure their input[4]. The lack of comprehensive internal diligence consultation with stakeholders in the face of surging demand for cloud computing drives an unnecessary and unhealthy wedge between stakeholders and leads to inconsistent decision-making. Such internal dynamics may well prevent optimal utilization of this new capability.

In my observation, enterprise cloud projects are far more likely to achieve optimal results when corporate counsels and other compliance stakeholders are fully involved in the due diligence process from the start. This article offers a tool and a process, based on a recently published international standard, to enable corporate counsels and other compliance stakeholders to conduct cloud due diligence systematically and consistently.

Structured due diligence tailored to each organization’s requirements is essential for cloud projects

Given the unrelenting growth in demand for cloud computing and the knowledge gap among corporate counsels and other compliance stakeholders about how to conduct cloud due diligence, there is a critical need for guidance material to help cloud customers structure their requirements. However, the prospect of a comprehensive framework for cloud migration decisions has been elusive because cloud requirements differ greatly depending on industries, geography, organizational culture, and specific project goals. For example, the security requirements for national critical infrastructure organizations are fundamentally different from those of retailers; the privacy regulatory requirements for European operations are different from those in the US; firms with heavy R&D investments have unique intellectual property protection needs; and required technical performance clearly differs from project to project.

A one-size-fit-all set of requirements will not work. What cloud customers need is a framework they can use to develop their own unique set of requirements to match external demands, organizational needs, and project technical requirements. The specifics of the requirements will differ. But there is no dispute that all cloud customers require a precise understanding of what their cloud providers will deliver in terms of privacy protection, security, regulatory compliance, and other key considerations. The unfortunate reality is that such requirements are often forgotten. The Forrester research cited earlier, for example, finds that regulatory and standard attestation is considered in only 36% of cloud agreements.

Answering the demands of the marketplace, the world’s leading standards bodies, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), have jointly developed a new international

standard, ISO/IEC 19086-1, to help organizations around the world specify their unique requirements for cloud migration.

ISO/IEC JTC 1: Where the world's most important technology standards are born

ISO and IEC's Joint Technical Committee 1 (JTC 1) is responsible for the development of vendor-neutral international technical standards in the Information and Communication Technology domain, including ISO/IEC 19086-1. Its members are national standards institutions, such as the American National Standards Institute (ANSI) for the United States and The British Standards Institution (BSI) for the United Kingdom. Since its creation 30 years ago, JTC 1 has created many critical standards that have influenced every corner of information technology, including the foundational ISO/IEC 27000 Information Security Management family. Since my focus is on cloud standards, I won't attempt to review the full spectrum of ISO/IEC JTC 1's work here, but interested readers should explore this vast area online[5].

The transnational nature of cloud computing makes the international harmonization that ISO/IEC brings critical. The many different stakeholders in the global cloud ecosystem require a shared understanding of the concepts and implementation details of cloud computing, even if they will inevitably have different views about what cloud services should or should not do with user data.

In broad terms, there are two kinds of international cloud standards:

- Standards that enable organizations to seek certification via self-attestation or third party audits of their internal processes. Prominent examples are ISO/IEC 27001 for Information Security Management and its associated ISO/IEC 27018 Code of Practice for the protection of personally identifiable information (PII) in public clouds.
- Standards that don't lead to certifications, but promote transparency in communication between providers and customers by establishing rigorous and detailed definitions for terms, reference architectures and frameworks. A key example is the ISO/IEC 19086-1 Cloud Service Level Agreement (SLA) Framework.

A brief history of the ISO/IEC 19086-1 standard for cloud SLAs

The specific subcommittee of ISO/IEC JTC 1 that produces 19086 (known as JTC1 SC38 WG3) counts participants from leading technology vendors such as IBM, Microsoft, Oracle, Amazon Web Services (AWS), Hitachi and Orange, as well as the standards bodies of 16 countries, including the United States, China, Japan, Korea, the UK, France and Australia. But the single biggest driver of the 19086 cloud SLA standardization process is arguably NIST, the U.S. National Institute of Standards. NIST is, in effect, the in-house standards department of the largest single purchaser of cloud services in the world, the U.S. Federal Government. Working with other U.S. agencies such as the General Services Administration (GSA) and the White House's Office of Management and Budget (OMB), NIST has for several years been leading a systematic effort to standardize and streamline the complex and inconsistent processes by which the Federal Government procures and deploys cloud services.

On the other side of the Atlantic, the European Commission has formed the Cloud Select Industry Group on Service Level Agreements (C-SIG SLA) to guide small and

ISO/IEC 19086 is a new international standard that will help organizations specify their unique requirements for cloud migration

medium businesses in their cloud purchase decisions. Like NIST, the work of C-SIG SLA has been influential in the development of ISO/IEC 19086-1.

These combined efforts are now coming to fruition and, thanks to their international and multi-sector amplification via ISO/IEC 19086-1, promise to become the foundation for cloud SLA standardization for all enterprise cloud customers, regardless of industry or country.

How stakeholders will use ISO/IEC 19086-1 to determine their cloud requirements

ISO/IEC 19086-1 sets out and defines a broad range of possible cloud service level objectives and cloud service qualitative objectives. Cloud service level objectives – or SLOs – are quantitatively measurable requirements, such as cloud availability, that can be expressed numerically. They are generally the concerns of the technical project team. Cloud service qualitative objectives – or SQOs – are requirements that cannot be expressed numerically. Examples include personally identifiable information protection requirements, law enforcement access policy, attestation to regulatory requirements, and methods and levels of customer support. Apart from a small number of exceptions such as customer support, the requirements of these cloud service qualitative objectives tend to be consistent across the enterprise regardless of the projects. These are generally the objectives where corporate counsels and compliance stakeholders should focus their attention.

Microsoft has developed a Cloud Services Due Diligence Checklist based on ISO/IEC 19086-1 customers can use for any cloud negotiations

To make it easier to navigate the cloud service level objectives and cloud service qualitative objectives from ISO/IEC 19086-1, a concise checklist is outlined in the appendix[6]. I urge readers to consult the standard in its original form[7] before applying it to an internal diligence requirement setting.

The application of the cloud service objectives in the standard for internal diligence requirement setting can be broken into three steps:

I. **Organizational Cloud Requirements Definition**, where industry, legal, and organizational requirements are defined and prioritized. The requirements and prioritization defined in this process should be reusable across all cloud projects within the organization, resulting in more consistency and robust due diligence. The involvement of corporate counsels and compliance stakeholders in this process is crucial.

II. **Project Requirements Definition**, where project-specific requirements are defined and prioritized. This is the step where cloud service technical features and cost constraints, which are not enumerated in ISO/IEC 19086-1, are defined. It is possible that project-specific requirements may conflict with the organizational requirement as defined earlier. In this case, reconciliation involving the appropriate stakeholder is necessary.

III. **Project Options Assessment**, where different architectural options or different cloud provider options are compared against the requirements and priorities as defined in previous steps.

I will only elaborate on step I, since the others are mostly the concerns of technology procurement. While corporate counsels and compliance stakeholders should still be involved in reconciling requirements as needed and assessing performance of different options in steps II and III, those are not particularly challenging, especially when step I is done well.

Here is an outline with a recommended five-step process for defining Organizational Cloud Requirements:

1. The process begins with an enumeration of the cloud service qualitative objectives and cloud service level objectives from the standard or the checklist. In table 1, I list only the first objective from ISO/IEC 19086-1, accessibility, for illustrative purposes. Accessibility refers to the design of products or services for people with disabilities. Equal access to cloud technology for people with disabilities can, in some jurisdictions and industries, be a regulatory requirement. In other cases, organizations may opt to go above and beyond in making cloud accessible even when there is no regulatory requirement. I will expand upon this later.
2. External requirements are those imposed on the organization by regulators or industry groups. Many multinational enterprises are exposed to a complex array of external requirements from different regulators in different countries. It may not be necessary to fully itemize all external requirements. The pragmatic pathway is to outline the most stringent and applicable requirements here. In the case of accessibility, some European governments, for example, require meeting the European public sector ICT accessibility procurement standard of EN 301 549. The requirement will differ for other industry sectors and jurisdictions. In some cases, the table cells may be empty because there is no external requirement. This is particularly likely for the more project-specific objectives, such as technical support or availability.
3. Organizational requirements are those which reflect the values and policies of the enterprise. In many cases, an organization may set voluntary policies that exceed the external requirements imposed upon it. Some jurisdictions do not have specific technical regulatory requirements or even anti-discrimination legislation related to accessibility. However, organizations can self-impose requirements to make their cloud technology accessible for employees and customers with disabilities. Again, not all objectives are applicable, especially those that are more project-specific.
4. The next step is to combine the external requirements with the organizational requirements. This is the common set of requirements for all cloud projects for the organization.
5. Lastly, some degree of prioritization should be set for each applicable requirement. This will ensure a degree of consistency from one cloud project to the next. I use a scale of 1 to 10 in this example. But other schemes can be suitable as well.

Table 1: Organizational Cloud Requirements Definition

STEP 1 **Objectives**	**STEP 2** **External Requirements**	**STEP 3** **Organizational Requirements**	**STEP 4** **Combined Organizational Requirements**	**STEP 5** **Prioritization**
Accessibility	EN 301 549	Same as 2	EN 301 549	Scale of 1 to 10
…				

The process outlined here, while simple on paper, can be a lengthy and complex process in practice and one that potentially involves outside counsel. However, the outcome of this exercise will be a deeper understanding of the organization's cloud policies and priorities. It is a roadmap to successful and rapid business process transformation through cloud computing.

Conclusion: Corporate counsels will evolve from legal gatekeepers to true business partners

> "ISO/IEC 19086 will help corporate counsels evolve from legal gatekeepers to true business partners."

The cloud revolution has taken enterprise IT and consumer technology by storm. The pace of change has been unprecedented and shows no signs of slowing down. In a few short years, most of the world's server-side compute power will have shifted from thousands of separate data centers operated by user organizations to perhaps only a few hundred hyper-scale cloud facilities that collectively house tens of millions of servers.

The reality is that we cannot expect corporate counsels to keep up with the rapid pace of technological change in cloud computing, which is likely to continue far into the future. The good news is that the internationally recognized ISO/IEC 19086-1 standard described in this article now offers corporate counsels a simple but thorough formal mechanism for ensuring that relevant privacy, security and regulatory requirements of proposed cloud projects have been identified, documented and complied with. Having such a tool in hand, corporate counsels will be able to step out of their traditional role of gatekeepers to become true partners who fully share and contribute to the business goals of their organizations.

Appendix A: ISO 19086 Cloud Service Agreement Objectives

Performance	
Accessibility	❑ List accessibility standards, policies, and regulations met by the service.
Availability	❑ The percentage of time that the service is available and usable.
Capacity	❑ The number of simultaneous connections. ❑ The maximum capacity of resources. ❑ The number of inputs that will be processed over a period of time. ❑ The amount of data that will be transferred over a period of time.
Elasticity	❑ How fast and how precise the service can adjust to the amount of resources that are allocated.
Service	
Service monitoring	❑ The parameters and mechanisms to monitor the service.
Response time	❑ The maximum, average, and variance in response time.
Service resilience/ fault tolerance	❑ The methods used to facilitate resilience and fault tolerance (include mean times, maximum times, and units of measurement).
Disaster recovery	❑ The maximum time required to restart the service in outage. ❑ The maximum time prior to a failure during which changes may be lost. ❑ The recovery procedures to restore the service and data.

Backup and restore data	❑ The number of data backups made in a period of time. ❑ The methods of backup and backup verification. ❑ The backup retention period. ❑ The number of backups retained. ❑ The location of backup storage. ❑ The number of restoration tests and the availability of test reports. ❑ The alternative methods for restoring data.
Cloud service support	❑ The available support plans, associated costs, and associated hours of operation. ❑ The specific contacts for service support. ❑ The service support methods (phone, web, tickets). ❑ For incident support: the incident support hours, levels of support, response time (average and maximum), reporting methods, and notification terms.

Data Management	
Cloud service provider data	❑ Define cloud service provider data.
Cloud service customer data	❑ Define cloud service customer data and usage terms.
Intellectual property rights	❑ Describe any intellectual property rights the cloud service provider claims on cloud customer data and vice versa.
Account data	❑ List the required account data fields (names, addresses, etc.).
Derived data	❑ Define the types of derived data and policies for use/access.
Data portability	❑ Data portability capabilities including methods, formats and protocols.
Data deletion	❑ Define the minimum and maximum times to completely delete cloud service customer data. ❑ Describe the data deletion process.

	❑ Describe the data deletion notification policy.
Data location	❑ List the geographic locations that data may be processed and stored, and if the cloud service customer can specify location requests.
Data examination	❑ Describe how the cloud service provider examines cloud service customer data.
Governance	
Roles and responsibilities	❑ The roles and responsibilities for the parties.
Personally identifiable information (PII)	❑ The PII protection standards met by the cloud service provider.
Information security	❑ The information security standards met by the cloud service provider.
Termination of service	❑ The process of notification of service termination, including the length of time that data and logs are retained after termination, the process for notification, and the return of assets.
Changes to features and functionality	❑ The minimum time between service change notification and implementation, and service change notification method. ❑ The minimum time period between the availability of a feature/function and the deprecation of that feature/function.
Law enforcement access	❑ The policy for responding to law enforcement requests of cloud service customer data.
Attestation, certification, and audits	❑ List/define the standards, policies, regulations, and applicable certifications that the cloud service provider attests to. Include audit schedule and location policies.

Notes

[1] Data in this paragraph are drawn from the Cisco Global Cloud Index annual research reports. For the current edition see http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html.

[2] Microsoft's Windows Server is the most widely used server operating system in enterprise computing. However, at Microsoft we also embrace open source. One third of the virtual machines in our Azure cloud run the open source Linux operating system.

[3] The full Forrester Research study is available at https://aka.ms/forrester.iso19086

[4] Dan Solove, "*Clearing Up the Fog of Cloud Service Agreements*"; https://www.linkedin.com/pulse/clearing-up-fog-cloud-service-agreements-daniel-solove

[5] See http://www.iso.org/iso/jtc1_home.html.

[6] The checklist also be download from https://aka.ms/cloudchecklist

[7] The standard is available from ISO at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67545 or IEC at https://webstore.iec.ch/publication/25920