Microsoft

Think Cloud Compliance

Achieving Trust and Compliance in the Cloud

International In-house Counsel Journal
Vol. 9, No. 36, Summer 2016, 1

Rich Sauer,
Corporate Vice President
and Deputy General Counsel,
Microsoft Corporation

The accelerating shift from traditional on-premises information technology ("IT") systems to cloud computing presents in-house counsel with a veritable obstacle course of compliance challenges and regulatory pitfalls. Virtually every industry today faces an expanding set of data security demands, while different countries often have their own unique privacy and data protection requirements. Even global regulatory landscapes can change with the stroke of a pen, as with the recent invalidation of the long-standing Safe Harbor data transfer arrangement between the EU and United States. Today's in-house counsel must master all of these requirements, explain them to their boards, and verify that their organization complies with them.

The cloud is all around us in modern enterprise computing. Here is a brief list of some common examples:

- Cloud email and productivity services: Microsoft Office 365, G Suite
- Full-fledged cloud-based business applications: Salesforce.com for Customer Relationship Management (CRM), Workday for Human Resources Management and ERP
- Cloud-based virtual servers that can be launched in minutes and operated on a pay-as-you-go basis for any business or web application: Amazon Web Services (AWS), Microsoft Azure, IBM Softlayer
- Cloud-based machine intelligence: Microsoft Azure, IBM Watson
- Cloud-based data storage that expands or contracts flexibly with requirements: Box, Dropbox

For a technology vendor, keeping a broad portfolio of feature-rich cloud services in compliance with an ever-changing regulatory landscape is—by definition—a never-ending challenge. At Microsoft, our own lawyers engage daily with our cloud engineering teams to help them understand and implement the requirements of this complex and evolving regulatory universe. This article will discuss Microsoft's experience working to meet the exacting legal and compliance requirements of our customers around the world.

By reviewing several particularly thorny regulatory and compliance issues that Microsoft has grappled with, this article also discusses several technical developments that in-house counsel need to understand as they evaluate cloud services. Our fundamental message is simple: the economic and strategic advantages of cloud computing make it impossible to ignore, but the transfer of responsibility over sensitive data and applications from customers to cloud providers requires the formation of a new framework for establishing and maintaining trust between these contracting parties.

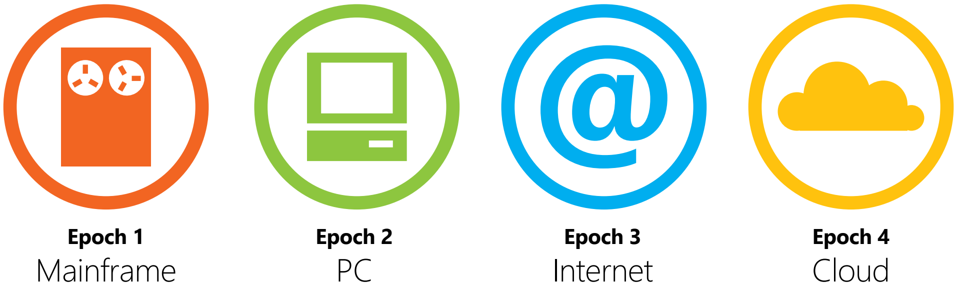
Every Business will be a Digital Business: Why the Cloud is Surging

After decades of unceasing progress in computers and software, we are all familiar with the tech industry's tendency to overhype each new innovation. Every press release seems to herald a new era, every product promises to change the world. But after a few months or quarters of excitement, the new technologies launched with great fanfare often turn out to be only incremental improvements, not revolutionary breakthroughs.

We all recognize that pattern. However, this innovation truly is different. The cloud really is a revolution, and it really will change the world. In fact, it is already doing so.

To understand why the cloud is different, we can divide the past half century of computing into four epochs. The first was the epoch of the mainframe, behemoths so big and expensive they could only function inside dedicated buildings owned by giant corporations. This epoch was dominated by IBM.

The four epochs of business computing



> "Although we think of the Internet as the foundation of our modern high tech world, in reality the Internet epoch was only a brief interlude."

The second epoch was that of the PC, launched in the early 1980s by Apple, Microsoft and Intel. These inexpensive desktop computers were first marketed to hobbyists and consumers, but soon swept the corporate world, penetrating into even the smallest organizations. By the 1990s, evolved versions of the PC known as servers also came to stand alongside mainframes in corporate data centers. But these servers still lacked the power to handle the most important "mission-critical" tasks.

By the latter half of the 1990s, the third epoch of computing emerged with the connection of hundreds of millions of client and server PCs into a vast global network. Known as the Internet, this network made possible countless new applications built on the reality that any individual could now instantly communicate with any other individual or access the information and processing power of any other computer on the planet.

Although we think of the Internet as the foundation of our modern high tech world, in reality the Internet epoch was only a brief interlude. Over the past few years, it silently mutated into something new, which we now call the cloud. This new epoch is a combination of the previous epochs, but innovations in software and hardware make the cloud almost unimaginably more powerful than previous computing paradigms. After the extreme decentralization of IT brought about by the PC and the Internet, the “cloud” is all about the recentralization of the world’s data and computing power into a relative handful of “hyper-scale” data centers. A single one of these facilities may house tens or even hundreds of thousands of PC-like servers packed into energy-efficient, massively interconnected racks spread out over the space of a football field or more.

The growth of the cloud in the early 21st century is strikingly similar to the rise of the electrical grid in the early 20th century. In 1905, when every factory needed to generate its own electricity on site, the United States counted 50,000 separate electrical power plants, typically using proprietary and incompatible standards. But within a few decades, even as the nation’s economy and electric power needs grew tremendously, 95% of those local plants had disappeared, replaced by a vast national grid where almost all power was generated in a few giant facilities.[1]

Today we are witnessing a similar transition in the organization of what we may call “information energy.” Within the next 10 years, the majority of business applications and virtually all consumer applications will be served from perhaps a few hundred of these huge cloud data centers, located in all of the world’s major geographies. Owing to its tremendous economies of scale, on-demand usage model, and pay-only-for-what-you-use billing, the cloud will progressively make inroads into the IT infrastructure of nearly all enterprises.

How confident should we be about rosy forecasts for the cloud’s future? As the father of quantum mechanics Niels Bohr once said, “Prediction is very difficult, especially about the future.” However, there is a clear and strong consensus among analysts that cloud growth forecasts are grounded in reality. Analyst firm Gartner estimates that global spending on commercial cloud services will pass $200 billion this year.[2] Investment bank Oppenheimer recently advised its Wall Street clients that the share of global compute capacity operated by the major cloud providers will likely approach 65% in the next five years.[3] Network manufacturer Cisco, whose equipment transports a large share of the world’s Internet traffic, estimates that cloud applications are growing 500% faster than traditional on-premises IT.[4]

$200 billion+

Global spending on commercial cloud services this year

—Gartner, Inc.

500% faster

Cloud applications growth compared to traditional on-premises IT

—Cisco Systems, Inc.

The Cloud is Transforming the Compliance Landscape

No one is predicting the complete disappearance of traditional in-house IT. On-premises IT systems will remain a vital part of enterprise computing for many years to come, especially to handle particularly sensitive data or mission-critical workloads. However, the cloud is disrupting even on-premises workloads. In the past decade, most enterprise IT organizations have embraced the software technique known as virtualization, which allows each individual hardware server to be shared by multiple “virtual” servers, thus yielding significant cost savings due to more efficient utilization of expensive capital equipment. Having first been virtualized, traditional on-premises data centers are now being “cloudified” by an additional layer of automation and management software that transforms these on-premises facilities into what industry analysts call “private clouds.”

> “…on-premises data centers are now being “cloudified” by an additional layer of automation and management software that transforms these on-premises facilities into…“private clouds.”

Large organizations are increasingly using private clouds to distribute internally generated “information energy” to their multiple business units, hoping to capture some of the flexible resource allocation and economies of scale offered by public cloud services. For instance, Microsoft offers a private cloud version of its public Azure cloud service known as Azure Stack. For customers using this software, servers and other computing assets in on-premises data centers are managed in much the same way that Microsoft operates the hardware and software in its public cloud data centers. Indeed, at the click of a mouse, customers can shift applications seamlessly from their private Azure cloud to Microsoft’s public cloud. In many cases, such readily hybridized private clouds will serve as a way station to the public cloud.

It is also true, of course, that the rise of the cloud does not mean distributed computing power will go away. On the contrary, the innumerable cloud applications and the oceans of information (including video, images, text, and quantitative data) that live in hyper-scale cloud data centers will be continuously connected via the Internet to many billions of end devices. The latter will include smart phones, tablets, PCs, and—last but not least—the oncoming tidal wave of "Internet of Things" sensors. But increasingly, the applications and services that make these devices useful will be powered by the cloud.

The economic and strategic benefits of cloud computing are too large for even the most risk-conscious organizations to forego. Indeed, because the cloud will increasingly be a strategic asset for innovation and productivity for companies across the economy, almost every business in the future will be a digital business.

But by shifting the permanent residence of data and applications to data centers owned by third parties that may be located in other countries or even on other continents, cloud computing introduces a level of legal complexity that requires a fundamentally new way of working and thinking by in-house counsel.

> “…cloud computing introduces a level of legal complexity that requires a fundamentally new way of working and thinking by in-house counsel.”

This article turns to these issues in the following sections. It begins with concrete examples of cloud computing and the compliance challenges it raises. It then reviews the types of cloud compliance issues that Microsoft has confronted on behalf of its customers. Finally, it comments briefly on how a large cloud provider like Microsoft conceives of compliance as an actual service that must be built to the same rigorous specifications as all our other products.

How the Cloud Raises New Compliance Challenges: The Example of Law Enforcement

When machines recognize faces and understand speech, we must pay extra attention to privacy.

In the past five years, researchers in universities and corporate R&D labs such as those of Microsoft, Facebook and Google have made dramatic progress in machine learning. Researchers now have a very good idea of how to build software that understands human speech and recognizes human faces. This field is moving more quickly than many people in the legal community may realize. In the past two years, such software has moved out of the research labs and into production in large consumer-facing applications such as Microsoft's Cortana digital assistant, Facebook's photo face tagging, and Google Photos. Now, machine learning is poised to break out of the consumer market and into the enterprise. Automated understanding of text, speech, images and video will very quickly become a standard feature of enterprise IT applications, from the most routine to the most strategic.

Training the models that power machine learning requires immense amounts of data and compute power. As a result, most production-caliber machine learning applications will have to reside in the cloud.

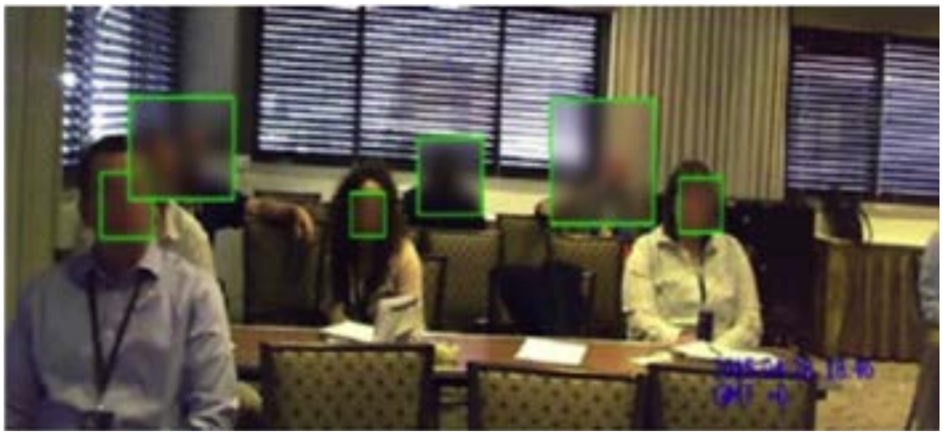
Question: When software in the cloud can understand the words and recognize the faces of vast numbers of individual users, what measures must enterprises and their cloud providers take to ensure compliance with legal mandates for privacy and the protection of personally identifiable information?

Because no single answer is sufficient, we have found it necessary to take a broad spectrum approach to developing situation-specific answers to this question and implementing those answers effectively in our cloud services. Privacy laws and regulations vary tremendously in their scope and definitions from one country or industry to another. Similarly, many different technical standards are relevant to the protection of personally identifiable information (PII).

A compelling example of why cloud providers need to deploy specific privacy standards to protect sensitive PII comes from a customer who recently chose to deploy its applications on Microsoft Azure. The customer is TASER, a well-known supplier of law enforcement equipment. In recent years, TASER has become the world's largest supplier of police body-worn cameras. Now being deployed in the thousands by law enforcement agencies across the United States and in other large markets such as the UK, these cameras generate enormous quantities of video data on a continuous basis. As a practical matter, the only affordable and technically feasible place to store this video data is in the cloud. This is why TASER made the decision early on to bundle its body-worn cameras with its own cloud video storage and retrieval service called Evidence.com.

Video from police body cameras is not inert matter. It is live evidence that is subject to strict legal rules governing access rights and the chain of custody. It must be readily searchable and made available for review by multiple participants in law enforcement cases, including investigating officers, prosecutors, defense attorneys, victims and their families, elected officials, and often the media. But by its nature, police video frequently records scenes of individuals in states of distress that are not suitable for unrestricted distribution to the public. Hence, law enforcement agencies using body cameras have found it essential to develop video redaction policies to protect the privacy and identities of individuals captured on video, particularly when these individuals are victims, innocent bystanders, or vulnerable witnesses.

But the obligation to redact police video prior to public disclosure (as mandated by law in many states) creates a new problem. It turns out that manual video redaction is a very labor-intensive process, one that is so expensive that some law enforcement agencies have been forced to halt body camera deployments due to lack of staff and budget for redaction. Here is where cloud-based machine learning comes in. TASER decided to use machine learning capabilities available on Microsoft Azure that—under the supervision of a human expert—automate video redaction by recognizing individual faces and tracking them through extended video sequences.



Automated Redaction of Faces in Police Video (image source: Microsoft)

Yet one vital question remained. If TASER was not only to store vast quantities of sensitive police body camera video in the Microsoft Azure cloud, but also to use machine learning to identify and track individuals in that video in order to protect their privacy, what standards would ensure that this data would not be subject to breaches or leaks? Although the video would be encrypted, TASER would still have to share the encryption keys with Microsoft in order for Azure's machine learning

> “Office 365 and Azure services were the first commercially available public cloud services to achieve CJIS compliance.”

algorithms to be applied to the data. Given this, what binding guarantees of conformity to rigorous standards could Microsoft offer TASER and TASER offer to its law enforcement customers that would assure the protection of data once it was transmitted from TASER’s premises to Microsoft’s data centers?

The answer to these questions lies in a little-known but crucial data protection standard specifically developed for sensitive law enforcement information. That standard is the FBI’s Criminal Justice Information Services (CJIS) Security Policy.

Half a dozen years ago, when the cloud was still in its infancy, cloud providers were not well-versed in the unique data protection requirements of law enforcement agencies. In several cases, police departments were forced to cancel deployments of cloud-based email services when they discovered that the services did not comply with the CJIS Security Policy. We at Microsoft knew that we were not immune to similar setbacks. Accordingly, we took these incidents as a wake-up call and initiated a multi-year journey that culminated in our Office 365 and Azure services becoming the first commercially available public cloud services to achieve CJIS compliance.

Meeting the CJIS standard required careful reengineering not only of the technical security features of our cloud services, but also of the business processes and personnel management practices in which those services are embedded. To cite just one example, the FBI’s demanding requirements specify that if employees of organizations providing services to law enforcement have access to protected data, they must pass rigorous criminal history background checks. Subjecting our data center personnel to such CJIS checks on a routine and institutionalized basis is an expensive process. However, we made the decision to accept this cost because we understood that it was an essential step towards meeting the needs of the broader state and local government community, of which law enforcement is only one—albeit crucial—part. Although the CJIS background checks are specific to our Government Cloud offerings in the United States, the business processes we developed to comply with this standard have had a positive spillover effect on all of our enterprise cloud services.

How One Cloud Provider is Meeting the Challenge of EU Data Protection Laws

Big data applied to personal information can readily fall afoul of EU data transfer rules

Big data analytics will revolutionize the ability of enterprises to understand exactly what is happening in their markets and how to shape future outcomes. Such methods require enterprises to store and analyze vast quantities of data—so vast that the accepted term is “data lakes.” Realistically, such “lakes” of data can only be stored in the cloud. Yet in many cases they will contain PII of customers and employees and will therefore fall under the strictures of data privacy laws, including the demanding new data protection laws recently passed by the European Union.

Question: How can multinationals doing business on both sides of the Atlantic ensure that their strategic big data analytics programs will not run afoul of rules governing international data transfers?

Answer: Multinationals should partner with cloud vendors who have spent years understanding what regulators require and how to implement both the technical and the legal components of a full-spectrum cloud compliance strategy.

At a time when technology has outpaced existing legal frameworks that govern how confidential data is protected, and when governments are struggling to balance public safety with the right to privacy, enterprises must work continuously to ensure that the services provided by their technology vendors retain the trust of all stakeholders—including governments, corporations and individual consumers. Recent events demonstrate just how complex this challenge can be for enterprises that operate in multiple jurisdictions.

In October 2015, the Court of Justice of the EU ("CJEU") abruptly invalidated U.S.-EU Safe Harbor Framework, which was based on a 15-year-old agreement between the United States and the European Commission that had enabled thousands of enterprises to move personal information across the Atlantic while remaining in full compliance with the EU's stringent data protection rules. But with the stroke of a pen, the CJEU threw the legality of transatlantic data transfers into doubt.

At Microsoft, we had long recognized that a sudden collapse of Safe Harbor was a possibility and had already taken steps to prepare for it. Starting in 2010, we assigned a dedicated team of several dozen lawyers and public policy professionals to the task of creating a new cloud contract based on the standard contractual clauses—often known as "model clauses"—that the Commission established pursuant to the EC's 1995 Data Protection Directive. Such an enhanced contract was not something we were required by law to offer, but we knew it would allow our customers to stay in compliance with EU law—at least provisionally—even without Safe Harbor.

Over a period of several years, our compliance experts met on numerous occasions with officials from the European Commission and the EU's 28 member-state Data Protection Authorities (DPAs) to hammer out a solution. In April 2014, the European DPAs determined that the Model Clauses in our new enterprise cloud contract met their requirements for a valid legal framework governing international data flows.[5] These clauses, which we now offer by default to all cloud customers of different sizes, ensure that even without Safe Harbor, all personally identifiable information stored in the Microsoft cloud continues to meet Europe's rigorous privacy standards no matter where it is located.

We undertook this complex and frankly quite expensive process because we knew that our cloud customers depend on their ability to use Microsoft services to transfer data across the Atlantic in a manner that complies with EU law. It was our job to anticipate future problems and to make certain that our customers could rely on stable and legally compliant cloud services, even in the face of an uncertain legal landscape subject to sudden tectonic shifts in prevailing regulatory regimes.

However, it is critical for compliance professionals and in-house counsel to understand that compliance will always remain a moving target.[6] The EC model clauses we introduced in our standard cloud contracts are themselves under challenge and may give way to new regulatory requirements. For example, the U.S. government and the EU have recently negotiated a new agreement called Privacy Shield to replace Safe Harbor. This is an important step toward creating a new legal framework to enable data to move between Europe and the United States in way that satisfies the data privacy and security concerns of both sides. The Privacy Shield has been ratified by the European Commission and all EU member states,[7] but it is nonetheless certain to be challenged in court.

Today, Microsoft is working with EU data protection authorities to ensure that its cloud services meet the requirements of the Privacy Shield. At the same time, recognizing that certain nations have data sovereignty requirements that go beyond Privacy Shield, Microsoft has also established data centers operated by trusted partners in countries such as Germany to offer customers an added layer of regulatory compliance assurance.[8]

Regardless of the outcome for Privacy Shield in its current form, it will be necessary for enterprises large and small to continue to grapple with changes in their legal and compliance requirements as they affect the use of cloud and other technology services. They should therefore actively seek out providers that will work to anticipate

Anticipating Compliance Changes

● **2000**
Safe Harbor decision established that U.S. company self-certification for storing customer data complied with EU Data Protection Directive

● **2010**
Microsoft starts developing "model clauses" as an added compliance safeguard without Safe Harbor

● **2015**
Safe Harbor invalidated by the Court of Justice of the EU (CJEU)

> "...it is critical for compliance professionals and in-house counsel to understand that compliance will always remain a moving target."

future legal and regulatory challenges and that are committed to deploying both the legal and engineering expertise needed to address these compliance challenges.

When Necessary, Cloud Providers Must Stand Up to Governments

A cloud provider's commitment to stand with its customers in matters of legal and regulatory compliance is every bit as important as its promise to offer the latest technical features and functionality. This commitment goes further than simply anticipating changes in the regulatory environment. When circumstances warrant, it also means that the cloud provider must be ready to challenge government actions in court that threaten the legitimate privacy and security interests of its customers.

> "We have not hesitated to challenge the U.S. government when we believed this was necessary to protect the interests of our customers and to preserve the rule of law."

At Microsoft, we have not hesitated to challenge the U.S. government when we believed this was necessary to protect the interests of our customers and to preserve the rule of law. In recent years, we have gone to court on multiple occasions to challenge government actions or demands that, in our view, exceeded what is permissible under existing law. In one of these cases, we won the right to disclose government requests for data held by our corporate customers. And while the vast majority of business users will never be the target of such a request, Microsoft fought to ensure that our customers' right to know what happens to their data is recognized and preserved as a matter of law and principle.

In a more recent case, the U.S. government demanded that Microsoft turn over emails of a customer who is not an American citizen and whose emails were stored in our data center in Dublin, Ireland. We believed that this unilateral attempt to exercise extraterritorial power to seize private information from a U.S. cloud provider operating overseas went beyond the intent of U.S. law and instead should have been pursued directly with the government of Ireland, in accordance with existing international agreements. We are proud to say that we received overwhelming support for our stand from many technology companies, legal experts, and privacy advocates, as well as from the government of Ireland and several members of the European Parliament.[9] On July 14, 2016, the United States Court of Appeals for the Second Circuit issued a historic decision in our favor, ruling that:

> *...the Stored Communications Act does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers.*[10]

Our willingness to stand up for the rule of law and the preservation of privacy extends to support for our competitors as well. In March 2016, we joined with a number of other leading technology firms to file a legal brief in support of Apple, as that company fought an FBI demand that it implement extraordinary measures to defeat the encryption on an iPhone used by one of the shooters in the terrible terrorist killings of December 2015 in San Bernardino, California.[11]

Of course, balance is essential in matters of public safety and national security. We take very seriously our responsibility to work with both American and foreign law enforcement agencies to help keep the public safe in accordance with the law. We have demonstrated this on a number of occasions by responding swiftly to urgent lawful requests for information. For example, when French police were pursuing fugitives following the Paris terrorist attacks in November 2015, we were able to turn over email data from the suspects' accounts within 45 minutes of receiving the request. But we also know that people won't use technology that they don't trust. Undermining these protections will only put us all at greater risk.

Microsoft quickly responded and legally turned over email data from suspects' accounts during Paris terrorist attacks in November 2015

Standards are Essential for Trust in the Cloud

The crux of the cloud compliance challenge lies in the fact that customers who choose the cloud must potentially place vast quantities of sensitive data into the hands of third parties whose facilities they do not control, often subject to the stringent regulatory requirements of specific sectors (banking, healthcare, government, consumer and employee PII, etc.). At the same time, customers must entrust these outside providers with the mission-critical business applications that process this data.

One might think that end-to-end data encryption or thorough onsite inspections of cloud provider data centers would mitigate some of the risks for customers. However, given the nature of cloud computing, neither encryption nor customer audits can provide a fully satisfactory response to the compliance challenge.

> “Neither encryption nor customer audits can provide a fully satisfactory response to the compliance challenge.”

Regarding encryption, while it is technically feasible for a user to encrypt data before sending it to the cloud and to ensure that the provider does not have access to the encryption keys, this approach is often not practical on a large scale. For example, while some large users in sensitive sectors do install special equipment to encrypt cloud-bound email, such encryption cannot conveniently be applied to email exchanged with correspondents outside the organization’s own firewalls, and in any case the metadata associated with the email (such as destination addresses) cannot itself be encrypted. Furthermore, sophisticated cloud-based algorithms such as machine learning, as well as security routines such as malware detection, cannot work on encrypted data thus limiting the value of the cloud for customers.

Allowing every customer the unfettered ability to conduct onsite inspections of cloud data centers would raise a host of practical challenges. At Microsoft, we have over 200 data centers around the world, including approximately a dozen that classify as true hyper-scale facilities. We subject all of these facilities to rigorous technical and business process engineering and regularly engage leading third-party auditing firms to ensure our compliance with literally dozens of formal standards. It would be impossible to manage thousands of customers continually arriving to inspect these sites and audit their regulatory compliance. To do so would, in fact, constitute a serious security risk that would be against the best interests of our customers.

Engagement of leading third-party auditing firms ensure compliance to literally dozens of formal standards

But the inadvisability of having individual customers audit cloud facilities points to the central importance of delegated trust provided by rigorous and widely recognized formal standards that are certified by independent third parties.

Examples of some of the many established standards Microsoft’s cloud services comply with[12]:

Global

- International Standards Organization: ISO 27001/2 (general IT security)
- ISO 27018 (protection of PII stored in the cloud)
- Cloud Security Alliance (Cloud Controls Matrix 3.0.1)

Regional or National

- Argentina’s PDPA
- Australia’s IRAP
- China’s MLPS
- Europe’s ENISA Information Assurance Framework
- Japan’s Cloud Security Mark

Industry/sector specific

- U.S. Federal Government’s FedRAMP
- Healthcare sector’s HIPAA
- Financial industry’s PCI-DSS
- Financial industry’s SOC 1
- Financial industry’s SOC 2

Virtually every one of these standards, and many others, require rigorous annual audits of our facilities or capabilities by accredited auditors. Complying with these multiple inspection and audit requirements is a resource- and time-intensive process that user enterprises would find extremely challenging to implement for their own data centers. In order to meet these requirements at Microsoft, we have created a

> “Microsoft has created a large dedicated organization of specialists whose full-time job is to manage the year-round standards audit activities that are continuously underway at our numerous data centers.”

large dedicated organization of specialists whose full-time job is to manage the year-round standards audit activities that are continuously underway at our numerous data centers.[13]

These teams must ensure coverage of complex requirement sets and manage frequent changes that result from the changing landscape of regulations, statutes, standards, and industry best practices for cloud services. As part of this work, we have created a standard methodology for defining compliance domains, determining which objectives apply to a given team or asset, and capturing how domain control objectives are addressed as they apply to a given set of industry standards, regulations or business requirements.

This highly structured approach is essential to giving us a clear understanding of the control activities that our cloud infrastructure teams must accomplish, the reasons behind each control activity (e.g., the specific clause from a requirements document such as SOC 2, or the specific element of security policy that drives the need to perform the control activity), as well as other functions that allow us to effectively manage our compliance programs. These programs also include frequent self-reviews performed by our internal teams and outside reviews of our overall performance against the control objectives. The reports prepared by third parties that conduct the regular audits of our cloud infrastructure provide a scalable mechanism for us to communicate our compliance capabilities to our customers and partners.

This compliance model extends to Microsoft’s consumer as well as enterprise cloud services, allowing for trusted third parties to examine service elements and provide detailed reviews of specific services such as Office 365 and Microsoft Azure. These independent assessments are logically stacked upon one another to reflect dependencies, and summary reports of these assessments are shared with our customers and partners.

We believe that this approach to managing our compliance program and control framework is essential if we are to continue to provide trustworthy cloud services.

Building a Framework for Trust

While cloud computing opens tremendous new opportunities, it also introduces great uncertainty. The same capabilities that make the cloud such a powerful enabler of commerce, connection and innovation can also be used to threaten our most fundamental rights and values. The bulk collection of personal information by U.S. and foreign intelligence agencies, recent terrorist attacks in the United States and Europe, the European Court of Justice decision to strike down the Safe Harbor Agreement—all these events raise important questions about privacy and safety, and make clear that technology needs to be governed by the international rule of law, not just the laws of physics and not just the laws of the United States.

At the heart of these questions lie matters of trust. As citizens, we want to trust that our governments can keep us safe and protect our right to privacy and free expression. As consumers, we expect technology to respect our preferences and keep its promises. As businesses, we need to be confident that we can serve our customers while obeying the laws of the countries in which we operate. For members of the legal and compliance community, trust is especially important to ensure that their clients meet regulatory obligations and community expectations while reaping the economic and strategic benefits of the cloud.

Microsoft's corporate mission—to empower every person and every organization on the planet to achieve more—depends on our ability to win and retain our users' trust. We strive to build trust through our commitment to principles that reflect timeless values that we share with all stakeholders. After long experience grappling with these issues, we reached the conclusion that such trust cannot be built in an ad hoc way. It must be built brick by brick on a deliberately designed and constructed foundation of first principles. After an extensive process of internal discussion and analysis, we have made the commitment to build all Microsoft cloud services on the following four fundamental pillars:

Security

Our priority is to safeguard your data with state-of-the-art technology, processes, and encryption.

Privacy and Control

Your data is your data, you own it, you control the privacy of your data, who has access to it, and where it resides.

Compliance

We will always offer the largest portfolio of compliance standards and certifications in the industry.

Transparency

You will always have complete visibility into where your data is located and how it's managed.

We believe that these principles and our commitment to them sets us apart. But we also know that we need to demonstrate exactly what these principles mean in practice for the legal and compliance community. And we understand that it is our responsibility to provide tools and information that will enable you to deploy our cloud services with the highest confidence that they are safe and compliant. For us, that is why compliance is a carefully engineered product, just like software code itself.

Our commitment to the legal and compliance community is deep and long-standing. It's the reason why Microsoft has more than 1,400 lawyers and public policy professionals working with legal and compliance leaders to help you tackle the regulatory issues you face in more than 100 countries where you and we do business.

> "Microsoft has more than 1,400 lawyers and public policy professionals working with legal and compliance leaders to help you tackle the regulatory issues you face…"

Our work on Model Clauses is not the only example of our commitment. We were the first cloud provider to offer Business Associate Agreements that enable healthcare organizations to comply with HIPAA. We were the first to meet the FBI's Criminal Justice Information Services data protection standard for law enforcement data. In education, we were the first major cloud provider to commit to the Future of Privacy Forum's Student Privacy Pledge. In the financial sector, we have done more to meet the exacting compliance needs of the world's biggest banks than any other technology company, which is one reason many of the world's leading financial institutions are adopting our cloud services.[14] And we were also the first cloud provider to achieve compliance with ISO's crucial new 27018 cloud privacy standard.

Trust is critical in your work and in ours. For your organization to succeed, you must be able to deploy technology solutions that your employees and your customers trust. And to fulfill our mission to empower every person and every organization, we know that earning your trust each and every day is critical. In the months and years ahead, we look forward to working in close partnership with you to achieve our common goal of ensuring that trust lies at the heart of technology.

Notes

1. "Cloud Surfing: A New Way to Think About Risk, Innovation, Scale, and Success," Tom Koulopoulos and Jim Champy, 2012.
2. "Global public cloud market expected to hit $204B in 2016," ComputerWorld, January 26, 2016 (http://www.computerworld.com/article/3026396/cloud-computing/global-public-cloud-market-expected-to-hit-204b-in-2016.html).
3. "AWS cloud computing ops, data centers, 1.3 million servers creating efficiency flywheel," ZDnet, June 7, 2016 (http://www.zdnet.com/article/aws-cloud-computing-ops-data-centers-1-3-million-servers-creating-efficiency-flywheel/).
4. "Backup, Virtualization, and the Next Big Thing: Cloud Workloads," Unitrends Blog (http://blogs.unitrends.com/backup-virtualization-and-the-next-big-thing-cloud-workloads-part-4/).
5. See "Privacy authorities across Europe approve Microsoft's cloud commitments," Microsoft President and Chief Legal Officer Brad Smith, April 2014 (http://blogs.microsoft.com/blog/2014/04/10/privacy-authorities-across-europe-approve-microsofts-cloud-commitments/#sm.0001fb0wq4aepf5at9510wnbemw62) and "Article 29 Data Protection Working Party Letter to Microsoft," April 2014 (http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf).
6. For a review of developments as of June 2016, see "Privacy Shield and the General Data Protection Regulation: More Key Developments," Sidley (http://www.sidley.com/news/2016-06-02-privacy-update).
7. See "Statement by Vice-President Ansip and Commissioner Jourová on the occasion of the adoption by Member States of the EU-U.S. Privacy Shield," July 8, 2016 (http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm).
8. For example, in November 2015 we announced plans to open two new data centers in Germany operated under an innovative "data trustee" model that guarantees data sovereignty under German and EU law. These new facilities will offer standard Microsoft cloud services such as Azure and Office 365, but will be under the control of T-Systems, a subsidiary of Deutsche Telekom, an independent German company acting as a data trustee. Microsoft will not be able to access this data without the permission of customers or the data trustee, and if permission is granted by the data trustee, will only do so under its supervision (https://news.microsoft.com/europe/2015/11/11/45283).
9. "Business, Media and Civil Society Speak Up in Key Privacy Case," December 15, 2014 (http://digitalconstitution.com/2014/12/business-media-civil-society-speak-key-privacy-case/).
10. U.S. Court of Appeals, "In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation," July 14, 2016 (https://consumermediallc.files.wordpress.com/2016/07/14-2985_complete_opn.pdf).
11. "Brief of Amici Curiae Amazon.com, Box, Cisco Systems, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, WhatsApp, and Yahoo in Support of Apple, Inc.," March 22, 2016 (http://images.apple.com/pr/pdf/Amazon_Cisco_Dropbox_Evernote_Facebook_Google_Microsoft_Mozilla_Nest_Pinterest_Slack_Snapchat_WhatsApp_and_Yahoo.pdf).
12. For a complete catalogue of standards implemented by our cloud services and extensive background information on each standard, see our recently launched cloud compliance portal at http://www.microsoftcloudassurance.com/.
13. For details of this process, see "Microsoft's Compliance Framework for Online Services" (download.microsoft.com/download/0/4/9/049F6894-3B22-4EC6-8DBD-E4FA27019820/Microsoft_Compliance_Framework_for_Online_Services.pdf).
14. For recent examples of how banks are working with our cloud services and dedicated compliance program for the Financial Services sector, see "Helping banks get more out of applications, the cloud and big data: Microsoft at Sibos 2015" (http://blogs.microsoft.com/transform/2015/10/15/helping-banks-get-more-out-of-applications-the-cloud-and-big-data-microsoft-at-sibos-2015) and "Transparency and assurance: How Microsoft is helping financial institutions move confidently to the cloud" (http://blogs.microsoft.com/transform/2015/10/13/transparency-and-assurance-how-microsoft-is-helping-financial-institutions-move-confidently-to-the-cloud).

MicrosoftCloudAssurance.com