Top Ten Security, Privacy and Compliance Questions to Ask Your Cloud Services Provider

May 2015

This whitepaper provides questions to consider when evaluating infrastructure and platform cloud service providers' security, privacy and compliance capabilities. For each question, the Azure response and guidance are provided so you can understand how Azure delivers security, privacy and compliance and how you can use Azure services to support your requirements and obligations.

Table of Contents

Question	Answer	Additional Guidance
Who can access my data?	Azure customers own and control their data. Azure uses use customer data only to provide the customers with the services to which they have subscribed, including purposes compatible with providing those services. As a service provider, Azure does not scan customer cloud services, applications, or data storage for advertising purposes. Additionally, Azure services incorporate the controls for ISO/IEC 27018 – an extension of the ISO 27001 standard with a code of practice governing the processing of personal information by cloud service providers. ISO 27018 controls reflect considerations for protecting personally identifiable information in public cloud services. ISO 27018 also provides clear guidance for cloud service providers for the return, transfer, and/or secure disposal of personal information of customers leaving their service. For more information, please visit the Privacy page on the Azure Trust Center.	Azure personnel can only access customer data under conditions contractually agreed to by customers on a "just-in-time" basis that is fully logged and revoked at the conclusion of the engagement. This is also referred to as "no standing access". Azure personnel do not maintain access to customer encryption keys, credentials, or other account information. • **Protections against inappropriate government access:** Microsoft has taken a firm public stand on protecting customer data from inappropriate government access and is actively driving its position through the courts. • **Protections against disclosure of customer data**: Microsoft will not disclose customer data to a third party (including law enforcement, other government entity or civil litigant) except as directed by the customer or required by law. If a third party contacts Microsoft with a demand for customer data, we will attempt to redirect the third party to request it directly from the customer. • **No broad access to customer data**: Except as the customer directs, Microsoft will not provide any third party direct, indirect, blanket or unfettered access to customer data. • **No access to encryption keys**: Except as the customer directs, Microsoft will not provide any third party the platform encryption keys used to secure customer data or the ability to break such encryption. In addition, customer data in Azure Storage (including SQL Database) is only accessible by the subscription owner by default; the option to provide access to other users through applications and services in their cloud environment is controlled fully by the subscription owner.

Question	Answer	Additional Guidance
		For more information about protecting data in Microsoft Azure, refer to this white paper. For Security Best Practices refer to this white paper.
What data privacy controls are in place?	Azure privacy controls reflect a superset of industry and regulatory requirements and practices that are enabled by default for all Azure customers. Azure enables customers to configure and manage privacy-impacting features to meet the needs of their organizations. • **Privacy Principles and Policies**: Microsoft has established privacy principles and privacy policies, which govern the collection and use of all customer and partner information. • **Privacy by Design:** Microsoft practices Privacy by Design, which describes how the company builds and operates products and services to protect privacy.	Azure maintains appropriate technical and organizational measures, internal controls, and data security practices to protect Customer Data against accidental loss or change, unauthorized disclosure or access, and unlawful destruction. Controls address logical network and storage isolation, options for data encryption, strong (multi-factor) authentication, certificate-based access controls, and detailed monitoring and logging. The Online Services Terms and its Data Processing Terms include our contractual commitment to privacy and security. For more information about data security and privacy, refer to the Azure Trust Center – Privacy and these whitepapers: • Protecting Data and Privacy in the Cloud • Protecting Data in Azure • Azure Network Security
What visibility do I have for where my data is stored?	Customers may specify the geographic area(s) ("geos" and "regions") of the Microsoft datacenters in which their customer data will be stored. In addition, Azure Storage maintains multiple copies of data to help guard against system or service failures, with replication across multiple physical disks and locations within the geo. The portability of data within Azure is what enables	Due to the nature of a shared-infrastructure platform such as Azure, data moves securely and freely between storage clusters based on customer geographic selection, size, traffic volume, and resource availability. If a failure were to occur that could impact customer data, the Azure Fabric would automatically re-allocate storage and move customer data transparently to available resources.

Question	Answer	Additional Guidance
	the platform to deliver high levels of scalability and service availability. Since Azure is a shared platform service rather than a provider of dedicated hardware, it is not feasible to identify a specific host or storage medium containing customer data. Portions of customer data could span multiple devices. The Azure service is the only means to access that metadata in the course of service delivery.	

What is your approach to security and how do you protect your environment from external attacks?	Microsoft believes that security, privacy, and compliance for its enterprise cloud services are a shared responsibility, with accountability distributed between Azure and the customer, depending on the service(s) being consumed. Azure helps customers reduce their security and compliance burden through trustworthy enterprise cloud services, offering the compliance capabilities customers need to help them fulfill their own standards or regulatory requirements (based on their use of Azure).
	
	Azure security spans physical datacenter facilities, hardware, infrastructure, operating systems, software, policies and controls, with audit and certification through independent third parties.
	
	There are two (2) broad categories of security features: 1) built-in security and 2) customer controls. Built-in security represents all the measures that Microsoft takes on behalf of all
		• Microsoft Antimalware is built into Cloud Services and can be enabled for Virtual Machines to help identify and remove viruses, spyware and other malicious software and provide real-time protection.
		• Azure uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits to protect against DDoS attacks.
		• Network isolation prevents unwanted tenant-to-tenant communications, and access controls block unauthorized users from the network.
		• Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Azure regions, and from Azure to on-premises datacenters.
		  ○ Azure ExpressRoute lets you create private connections between Azure datacenters and your on-premises infrastructure.
		  ○ Azure provides multiple capabilities for protecting data in-transit and at-rest, including encryption for data, files, applications, services, communications, and drives.
		• Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory

Question	Answer	Additional Guidance

	cloud customers to protect the Cloud environment to run a highly available platform and services. Azure development adheres to the Security Development Lifecycle (SDL) with security requirements embedded in systems and software through the planning, design, development, and deployment phases.
	Azure adheres to a rigorous set of security controls that govern operations and support and demonstrate compliance with industry and regulatory standards. Customer controls are features that enable customers to configure and manager their Azure subscription and environment to meet their organization's specific needs.
	
	Microsoft applies "assume breach" strategy to harden cloud services. A dedicated "red team" of software security experts simulate real-world attacks at the network, platform, and application layers, testing Azure's ability to detect, protect against, and recover from breaches.
		services, advanced identity governance, security, and application access management.
		• Azure Multi-Factor Authentication reduces organizational risk and helps enable regulatory compliance by providing an extra layer of authentication, in addition to a user's account credentials, and to secure employee, customer, and partner access.
		• Security reports are used to monitor access patterns and to proactively identify and mitigate potential threats. Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made.
		• Integrated deployment systems manage the distribution and installation of security updates for the Azure service.
		• Microsoft conducts regular penetration testing to improve Azure security controls and processes.
		• The Azure Marketplace provides access to dozens of third-party add-on security products and services for the cloud.
		• For additional information, see:
		  ○ Microsoft Security Development Lifecycle
		  ○ Operational Security for Online Services

Can we get our data out of your service?	Customers own their data and retain all rights, title, and interest in the data they store within Azure. Customers can download a copy of all of their data at any time and for any reason, without any assistance or notification required from Microsoft. For more information, please visit the Frequently Asked Questions page in the Azure Trust Center.	Customers have options with a variety of mechanisms to retrieve data from Azure. These include: • Standard file transfers of VHDs or individual files, or bulk copy via a dedicated high-speed private link such as ExpressRoute • Making backups of cloud data to your on-premises storage using Azure Backup or other mechanism such as StorSimple • Using the Azure Import/Export service to ship physical drives for Azure operations personnel to download your data

Question	Answer	Additional Guidance
		• Replicating data to your on-premises storage, including Active Directory and SQL data. In addition, when customers delete data or leave Azure, Microsoft follows industry best-practices for overwriting storage resources before reuse, and physical destruction of damaged or decommissioned storage devices according to guidelines set forth in NIST 800-88.
Will you let us know if our data / applications are compromised?	The security controls and risk management processes Microsoft has in place to secure Azure infrastructure reduce the risk of security incidents, but in the event an incident is suspected or were an incident to be confirmed, the Security Incident Management (SIM) team within the Microsoft Online Security Services & Compliance (OSSC) team operates globally 24/7 to respond. The team is responsible for assessing and mitigating computer security incidents involving Microsoft's Online Services, and managing any internal and customer communications. Microsoft makes contractual commitments regarding customer notification after we become aware of any unlawful access to customer data stored on our equipment or in our facilities, or unauthorized access to that equipment or facilities resulting in loss, disclosure, or alteration of customer data. Additional information can be found in Microsoft's Online Service Terms.	An important part of Microsoft's security capabilities is our response process. The Security Incident Management (SIM) team responds to potential security issues when they occur, operating around the clock. The SIM processes are aligned with ISO/IEC 18044 and NIST SP 800-61. There are six phases to the SIM incident response process: • **Preparation** – SIM staff undergo ongoing training to be ready to respond quickly and effectively when a security incident occurs. • **Identification** – looking for the cause of an incident, whether intentional or not, often means tracking the issue through multiple layers of the Microsoft cloud computing environment. SIM collaborates with members from internal Microsoft teams to diagnose the origin of a given security incident. • **Containment** – once the cause of the incident has been found, SIM works with all necessary teams to contain the incident. Containment methods are based on the business impact of the incident. • **Mitigation** – SIM coordinates with relevant product and service delivery teams to reduce the risk of incident recurrence. • **Recovery** – continuing to work with other groups as needed, SIM assists in the service recovery process. This phase often includes suggestions and recommendations for additional monitoring and penetration testing to validate mitigation efficacy. • **Lessons learned** – after resolution of the security incident, SIM convenes a joint meeting with all involved personnel to evaluate the

Question	Answer	Additional Guidance
		event and to record lessons learned during the incident response process.
Are you transparent with the way you use and access our data?	Access to customer data is strictly controlled and logged, and audits are performed by both Microsoft and third parties to attest that access is only for appropriate business purposes. Microsoft does not mine customers' data for marketing or advertising purposes. Azure enables customers to control and manage reporting on access to their customer data whether by their own administrators or users. Log data is also available on access by Microsoft support personnel.	Microsoft undergoes regular verification by third-party audit firms and shares audit report findings and compliance packages with customers to help them fulfill their own compliance obligations. By verifying that its services fulfill compliance standards and demonstrating how compliance was achieved, Microsoft makes it easier for customers to rely on Azure to support compliance for their infrastructure and applications that run in Azure.
What kind of commitments do you have with respect to security and privacy?	Microsoft is unique among major cloud service providers in providing cloud service-specific privacy statements and making strong contractual commitments to safeguard customer data and protect privacy. These include the Online Services Terms and its Data Processing Terms as well as the HIPAA Business Associate Agreement (BAA) for in-scope services. Microsoft also makes the standard contractual clauses created by the European Union (known as the "EU Model Clauses") available to enterprise customers to provide additional contractual guarantees concerning international transfers of personal data.	The following contractual commitments are backed by technical capabilities and operational practices that help ensure Azure fulfills privacy obligations, benefiting customers in every geography and industry. Customers across the globe can use Azure with confidence, knowing that Microsoft supports the high bar of privacy protections mandated by these regulations. Contractual scope includes: • Data Processing Terms that support our compliance with the E.U. Data Protection Directive • E.U. Standard Contractual Clauses that provide additional contractual guarantees around transfers of E.U. personal data outside of the European Union • A HIPAA BAA for healthcare entities that include Protected Health Information (PHI) in their customer data.

Question	Answer	Additional Guidance
How do you ensure that your service is reliable?	Azure is built using enterprise technologies that have evolved for more than two decades and is deployed in datacenters that support some of the biggest online properties in the world. Microsoft Online Services apply best practices in design and operations, such as redundancy, resiliency, distributed services, and continuous monitoring. Azure also demonstrates effective control design and execution for business continuity and disaster recovery, and commits to service level agreements. Azure maintains multiple distributions of data – in accordance with customer geolocation choice, across data centers, for redundancy.	Delivering services at huge scale requires a radically different approach to designing, building, deploying and operating datacenters. When software applications are built as distributed systems, every aspect of the physical environment — from the server design to the building itself — creates an opportunity to drive systems integration for greater reliability, scalability, efficiency and sustainability. Customers can take additional steps to protect their data by configuring Fault Domains, running regular backups, implementing backup and recovery services, and designing redundancy features for cloud applications and services. For more information on Microsoft's resilient software strategy and how cloud workloads have changed the way we design and operate datacenters, please read the Cloud-Scale Datacenter strategy brief and listen to our cloud engineer's presentation.
What are your service uptime commitments and capabilities?	Azure offers 99.9% uptime via a financially-backed service level agreement. If a customer experiences monthly uptime that is less than 99.9%, we compensate that customer through service credits.	Azure provides four (4) categories of business continuity / disaster recovery (BCDR) capabilities, and is regularly tested and subject to independent third party audit to verify effective control design and execution to support highly available, redundant services 1. **Recovery from local failures:** Physical hardware (for example drives, servers, and network devices) can all fail and resources can be exhausted when load spikes. Azure maintains high availability through load balancing, partitioning, replication, and elasticity. 2. **Recovery from loss of an Azure region:** Widespread failures are rare but possible, so Azure has accounted in our design that entire regions can become isolated due to network failures, or be physically damaged due to natural disasters. Customers can use Azure's capabilities to create applications that span geographically diverse regions by configuring failover clustering, geo-redundant storage, database mirroring (for SQL Server data), and regular backups.

Question	Answer	Additional Guidance
		3. **Recovery from on-premises to Azure:** The cloud significantly alters the economics of disaster recovery, making it possible for Customers to use Azure to establish a second site for recovery with a low barrier to implement and operate. Extending on-premises datacenters to the cloud through VPN, encrypted cloud storage (via StorSimple), Azure Backup, and SQL Database replication provides reliable mechanisms to support continuous application and data availability. 4. **Recovery from data corruption or accidental deletion:** Customer applications may have bugs which could corrupt data, or their administrators and users could inadvertently delete important data. Azure provides customers with the ability to back up data and restore to a previous point in time with blob snapshots for Azure Storage, as well as SQL Database import / export services. Additional information can be found in Microsoft's Online Service Terms.