KEEPING YOU SECURE

Compliance and Data Security

Property Information Exchange Ltd

poweredbypie

poweredbypie hosts in the Microsoft Azure Cloud for compliance and data security.

The benefits associated with the use of Azure are plentiful but include a reduction in costs and complexity, a reduction in risk associated with security, and risks surrounding compliance in the cloud. Recent studies have addressed some of the concerns felt by many when migrating to the cloud and concluded that rather than compromising security, cloud computing has significant security benefits; this is due to the high standards of technology and operational processes that Microsoft employ around their services. This cannot be easily matched by non-cloud technology, managed by other providers. Microsoft's can boast that the safeguarding of its enterprise cloud services complies with global standards. Furthermore, Microsoft's experience in running compliant online services means that the cloud customer can benefit from their expertise.

Infrastructure

There are several ways that Azure protects its clients' infrastructure. This ranges from protection of the physical datacentre, the hardware and software, networks, to staff, both administrative and operational.

Physical security is paramount and each datacentre is designed to run 24/7, employing measures to ensure protection against a range of disasters – including physical intrusion, power interruptions, and network outages. The centres comply with industry standards for security (ISO 27001) and availability. Microsoft personnel manage and monitor each centre.

Monitoring and logging is centralized. The devices generate a large amount of information and Microsoft employ detailed analysis and correlation in order to provide continuous visibility to clients and give timely warnings to in-house teams.

Update management helps to protect systems from known vulnerabilities and uses integrated deployment systems for installation and distribution of security updates for Microsoft software. Azure conducts thorough and regular database, operating system and web application scans of the entire environment using a combination of Microsoft's own tools as well as third-party tools.

For protection against virus and malware, all Azure software components are subjected to a virus scan prior to deployment. This ensures that all code moved to production has a clean and successful virus scan. Microsoft provides native anti-malware on all Azure virtual machines and recommends running some form of anti-malware or antivirus on all VMs. Each VM can be periodically reimaged to ensure all intrusions are eliminated.

Penetration testing to improve Azure security controls and processes is conducted regularly. Microsoft's policy on security assessment is that it is an important part of application development and deployment. They have therefore decided to carry out authorized penetration testing on their own applications hosted in Azure. This gives them, as administrators, useful information to ensure the safety of client applications.

Azure has DDoS (Distributed Denial of Service) protection as standard across its Azure platform services. It uses standard detection and mitigation techniques to detect and protect against these attacks. This system is designed to withstand attacks generated from outside the platform, as well as inside.

Network protection

Azure's shared infrastructure is responsible for many millions of virtual machines so protecting the confidentiality of its traffic is of the utmost importance to Microsoft. Azure differs to the traditional datacentre in that the responsibilities for network protection and management are shared between the provider and the customer, rather than the IT organisation. Customers are tasked with implementing the logical equivalent to their traditional security measures within the cloud environments. This would include the Virtual Private Network (VPN) administration, and security rules and firewalls.

Microsoft concedes that multiple deployments might be stored on the same piece of physical hardware. In order to isolate each customer, they use logical isolation techniques like Virtual Local Area Networks (VLANs) and virtual machines. This effectively segregates one organisation's data from another.

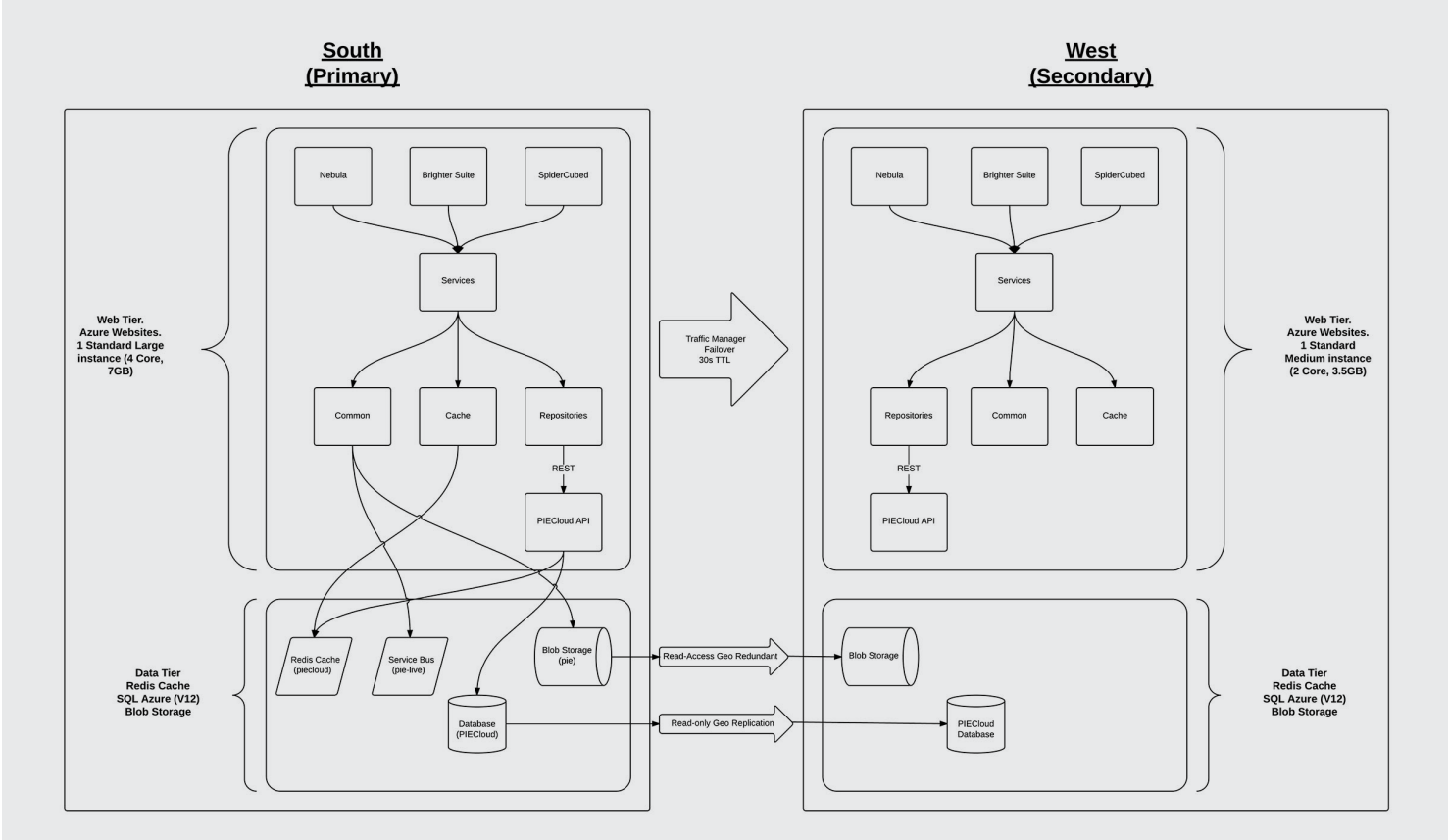
Using private IP addresses, multiple deployments may communicate with each other upon arrangement of a subscription. Otherwise, each VLAN remains isolated from the other. VPNs can be deployed to allow connections from customer sites and remote workers to access the data they need. Additionally, clients can use ExpressRoute, which keeps their traffic off the internet by using a fibre link directly to the datacentre. This is the route with the best performance.

Azure encrypt all communications across their networks using industry standard cryptographic technology. This enables the encryption of communications both within and between local services as well as between geographically separate datacentres.

In terms of Data Protection, Azure also allows encryption and key management using a wide range of methods, specifically chosen by the customer for their individual needs. These methods include Azure Key Vault, which is a cost effective and simple key management system for cloud based applications. Naturally, Azure's transport protocols meet industry standards. One such protocol is TLS which protects data in transit both between and within their datacentres.

Should **poweredbypie** decide to migrate from Azure to another hosting provider, Microsoft follow stringent standards for the overwriting of data in reallocation of the storage previously used.

Furthermore, customers can opt for in-country storage for compliance reasons or with disaster recovery in mind. Azure can ensure the replication of data inside of a selected geographical location. The below diagram illustrates how **poweredbypie** have implemented their UK primary and secondary application verticals exploiting in-country storage and replication to achieve localized compliance and resilience.



Identity and Access

Customers of Azure control access to their deployments. This ensures that access to the environments is limited to chosen internal personnel only. At Microsoft, employees have restricted access to the customer's deployments. Azure employs a package for access control: Azure Active Directory, which is a cloud-based access management solution. This solution governs members with access, manages the directory of active members, administers access to applications and provides security for current members. This ensures developers are able to build their own policy-based access rules for their applications. The scale of this solution is such that it meets the standard of enterprise level organisations, providing multi-factor authentication (MFA) and safeguarding access to data in compliance with regulatory standards. MFA can be employed using verification options selected by the user, such as email, phone, text or through a mobile application.

Azure's software generates security reports to allow customers to monitor access to their environments, as well as mitigating threats. Any access to the environments by Microsoft operations are also logged. Customers can also switch on additional monitoring tools for security, monitoring and threat detection.

Privacy

Microsoft's policy on privacy is detailed in the document "Privacy by Design". This details how they, as an organisation, build and operate their products to protect the customer's privacy. For specific practices, we can refer to their list of policies but below is an overview.

Firstly, Microsoft have a contractual commitment to customer's privacy, assuring the built-in protections for all users. Microsoft support the EU Model Clauses which regulate the transfer of EU customer data outside of the EEA. They also commit to the SCC (Standard Contractual Clauses) providing guarantees of privacy around transfers of personal data. Europe's privacy regulators have deemed Microsoft's delivery of these commitments as meeting EU standards, making Microsoft the first cloud-based provider to be deemed so.

In addition to the above, Microsoft also follows the US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Program. These are set forth by the US Department of Commerce regarding the collection, use, and retention of data from the EEA and Switzerland, ISO/IEC 27018. They also conform to the guidelines developed by the British Standards Institution. Of all the cloud providers, Microsoft was the first to adopt the international code of practice for cloud privacy. This code, ISO/IEC 27018, was developed to ensure a consistent approach globally to protecting the privacy of data in the cloud. It does this by putting controls in place that prohibit the use of customer data for marketing without the customer's express consent.

As previously mentioned, even Microsoft personnel have restricted access to customer data, and this access is carefully monitored by logs. They are authorised to access customer data only when it is necessary to support the customers. This could take place when troubleshooting or detecting problems reported by customers. On the occasion that access is granted to personnel, it will be revoked as soon as it is no longer needed.

Microsoft operates on the premise that customers should have control over where their data is stored; in the cloud or at a datacentre. They have a policy of not disclosing data to law enforcement officers unless required by law to do so or directed to by a customer. When they make disclosures, they aim to maintain transparency and ensure that only the data requested is provided, ensuring the privacy of the remainder of the data. If governments request customer data, it will only be provided if it has been subject to the appropriate legal processes and Microsoft has been issued a warrant or a subpoena. Unless prohibited to do so, Microsoft will inform the customer in question and provide them with a copy of the legal documents. Under no circumstances will Microsoft ever grant indiscriminate access to customer data and all requests will be reviewed by Microsoft's legal team to ensure their validity. Move details about this policy can be found in the Law Enforcement Requests Report provided by Microsoft, where they publish details of the number of requests they receive.

The anxieties around relocating data to the cloud are understandable and organisations may have concerns around data ownership. Microsoft, however, make it clear that customer data is owned and controlled by the customer regardless of where the data is stored. This sets Microsoft apart from other major cloud providers. This data is defined by Microsoft as “all data, including all text, sound, video or image files, and software that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service.” This would include any data uploaded by the customer for storage or processing as well as applications that the customer hosts in Azure. This also includes any information about administrators (including account contact and subscription administrators) supplied during signup, purchase, or administration of Azure, such as name, phone number, and email address. Additionally, metadata is owned exclusively by the customer. This extends to metadata like disk configuration settings, database settings and encryption keys. Azure also monitors access to control data such as passwords, security certificates, and other authentication-related data.

Due to the scale of Microsoft’s operations, customers are able to specify the geographic location where their data will be stored. This can also be replicated within a selected geographic area for redundancy purposes, but will not be replicated outside of it for redundancy.

Customers are given the option to manage and select their own encryption keys in order to ensure they have full control over encrypted data. The customer retains the right to authorize use of said keys and to revoke Microsoft’s copy of the key. If they do make the decision to revoke the key from Microsoft, it may impair the effectiveness of Microsoft’s troubleshooting and problem repair services.

Using role based access controls, Microsoft are also able to allow customers to restrict data access based on assignment of roles to groups of users. This is supported by Microsoft’s tools in Azure.

Compliance

In terms of compliance, Microsoft can boast of having the most comprehensive set of industry-recognised certifications. This makes them robust and forward thinking in this field. Their framework for compliance for online service map controls meet regulatory standards and this practice feeds into every new datacentre build, ensuring compliance of current operations as well as those in the future. This makes it easier for customers to ensure they meet compliance standards across the board as their own needs change, and demonstrate as much. These processes, along with the security tools that Microsoft employ, qualifies them for a range of third-party certifications which help customers demonstrate compliance to their regulators and consumers alike. Microsoft share results of third party assessments with customers. For more detailed information on Compliance, you can refer to Azure’s list of certifications and attestations. The list shows that Azure meets a broad set of international and industry specific standards, as well as regional standards where appropriate. These include ISO 27001, FedRAMP, SOC 1 and SOC 2.

Microsoft's continued commitment to adhering to the security controls detailed within these standards is verified by numerous third-party audits, proving that Azure meets world-class industry standards, certifications and attestations. Their strategy helps customers address business objectives and industry standards and regulations.

These assessments involve rigorous test and audit phases, security analytics, risk management best practices, and security benchmark analysis.

Microsoft Azure offers the following certifications for all in-scope services:

UK G-CLOUD - The UK Government G-Cloud is a cloud computing certification for services used by government entities in the United Kingdom. Azure has received OFFICIAL accreditation from the UK Government Pan Government Accreditor.

CDSA - The Content Delivery and Security Association (CDSA) provides a Content Protection and Security (CPS) standard for compliance with anti-piracy procedures governing digital media. Azure passed the CDSA audit, enabling secure workflows for content development and distribution.

CJIS - Any US state or local agency that wants to access the FBI's Criminal Justice Information Services (CJIS) database is required to adhere to the CJIS Security Policy.

CSA CCM - The Cloud Security Alliance (CSA) is a non-profit, member-driven organization with a mission to promote the use of best practices for providing security assurance within the cloud. The CSA Cloud Controls Matrix (CCM) provides detailed information about how Azure fulfils the security, privacy, compliance, and risk management requirements defined in the CCM version 1.2, and is published in the CSA's Security Trust and Assurance Registry (STAR).

EU model clauses - Microsoft offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU. Microsoft is the first company to receive joint approval from the EU's Article 29 Working Party that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. This ensures that Azure customers can use Microsoft services to move data freely through their cloud from Europe to the rest of the World.

FDA 21 CFR Part 11 - The US Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11 lists requirements for the security of electronic records of companies that sell food and drugs manufactured or consumed in the United States. The compliance reports produced by Azure's independent third party SSAE and ISO auditors identify the procedural and technical controls established at Microsoft and can be used to satisfy the requirements of CFR Title 21 Part 11. Microsoft is able to show how relevant controls within these reports have an impact on compliance with the FDA 21 CFR 11 regulations.

FedRAMP - Azure have Provisional Authority to Operate (P-ATO) from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) at a Moderate impact level based upon the FIPS 199 classification. FedRAMP is a US government program providing a standard approach to security assessment, authorization, and monitoring for cloud services used by federal agencies saving tax payers and organizations the time and cost of conducting their own independent reviews.

FERPA - The Family Educational Rights and Privacy Act (FERPA) is a US federal law that protects the privacy of student educational records. Microsoft agrees to use and disclosure restrictions imposed by FERPA.

FIPS 140-2 - Azure complies with the Federal Information Processing Standard (FIPS) Publication 140-2, a US government standard that defines a minimum set of security requirements for products and systems that implement cryptography.

HIPAA - The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that regulates patient Protected Health Information (PHI). Azure offers customers a HIPAA Business Associate Agreement (BAA), stipulating adherence to certain security and privacy provisions in HIPAA and the HITECH Act. To assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.

IRAP - Azure has been assessed against the Australian Government Information Security Registered Assessors Program (IRAP), which provides assurance for public sector customers that Microsoft has appropriate and effective security controls.

ISO/IEC 27018 - Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.

ISO/IEC 27001/27002:2013 - Azure complies with this standard, which defines the security controls required of an information security management system.

MLPS - Multi-Level Protection Scheme (MLPS) is based on the Chinese state standard issued by the Ministry of Public Security. Azure operated by 21Vianet adheres to this standard, which provides assurance for both the management and technical security of cloud systems.

MTCS - Azure has achieved Level-1 certification with the Multi-Tier Cloud Security Standard for Singapore (MTCS SS), a cloud security standard covering areas such as data security, confidentiality, business impact, and operational transparency, developed under the Singapore Information Technology Standards Committee.
PCI DSS - Azure is Level 1 compliant with Payment Card Industry (PCI) Data Security Standards (DSS) version 3.0, the global certification standard for organizations that accept most payments cards, as well store, process, or transmit cardholder data.

SOC 1 and SOC 2 - Azure has been audited against the Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2. Both reports are available to customers to meet a wide range of US and international auditing requirements. The SOC 1 Type 2 audit report attests to the design and operating effectiveness of Azure controls. The SOC 2 Type 2 audit included a further examination of Azure controls related to security, availability, and confidentiality. Azure is audited annually to ensure that security controls are maintained.

TCS CCCPPF - Azure operated by 21Vianet is among the first cloud providers in China to pass the Trusted Cloud Service certification developed by the China Cloud Computing Promotion and Policy Forum (CCCPPF).

poweredbypie

WYVOLS COURT
SWALLOWFIELD
RG7 1WY

DIRECT LINE
0800 038 8350

EMAIL ADDRESS
info@**poweredbypie**.co.uk

VISIT US
poweredbypie.co.uk

poweredbypie, Wyvols Court, Swallowfield, Reading RG7 1WY info@poweredbypie.co.uk poweredbypie.co.uk