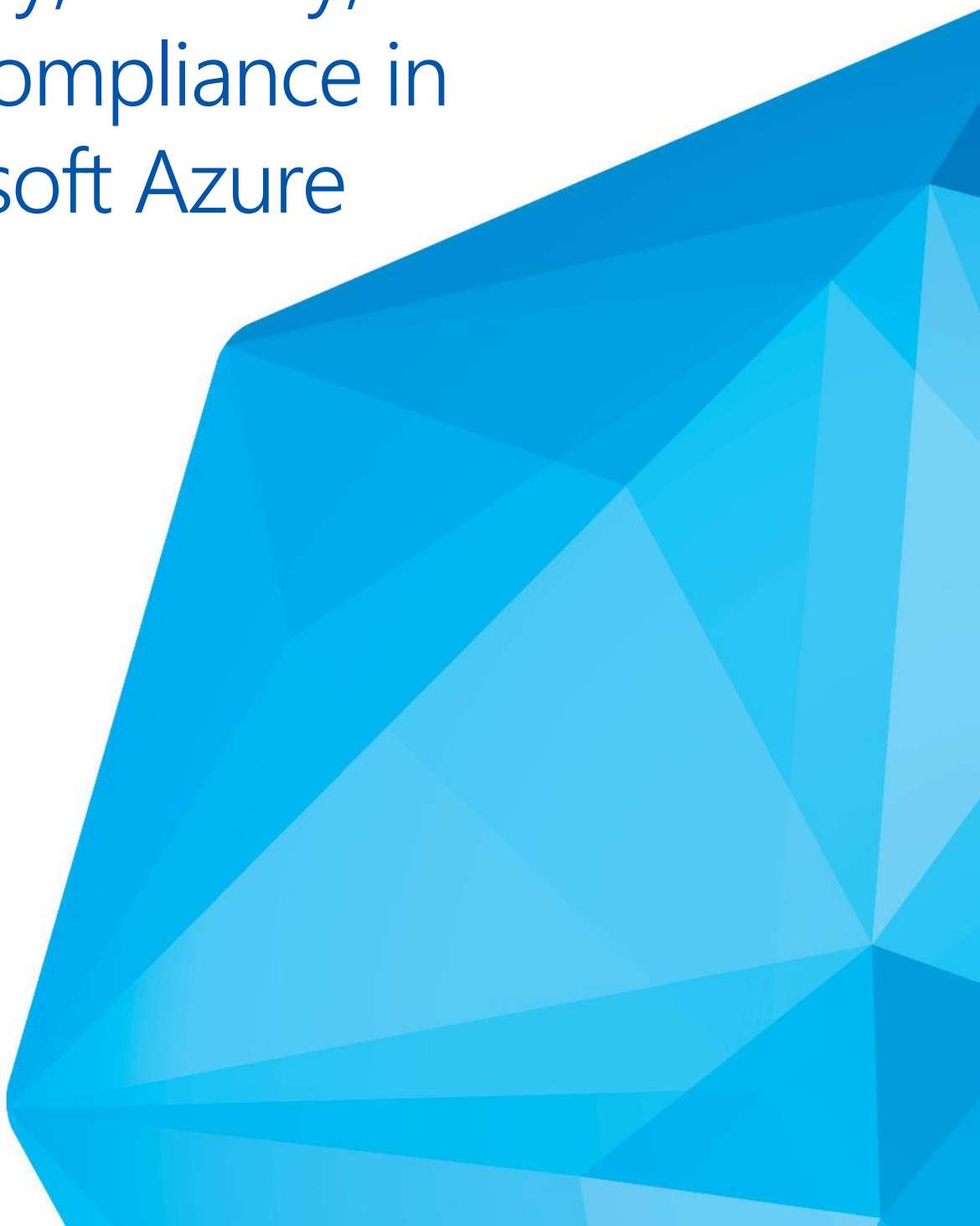
Microsoft Azure

White Paper

Security, Privacy, and Compliance in Microsoft Azure



Executive Summary

The adoption of cloud services worldwide continues to accelerate, yet many organizations are wary of trusting a third party with their data, applications, and infrastructure. Microsoft Azure helps customers achieve the economic benefits of cloud services while furthering security and compliance through:

- **Experience and innovation** providing trustworthy software and services, resulting in a foundation on which customers can easily build their own secure and compliant solutions.
- **Shared responsibility** that shifts some of the burden for implementing technical safeguards and operational processes to Microsoft while still providing the tools and flexibility organizations need to manage the service in accordance with their security standards.
- **Transparency** and third-party verifications to provide insight into Azure security controls and confidence that compliance standards are being met.

With Azure, organizations can benefit from Microsoft's industry-leading approach to security, privacy, and compliance while minimizing cost and complexity.

Introduction: The Advantages of the Right Cloud Services

According to an IDC study[1], 70% of CIOs will embrace a cloud-first strategy in 2016, meaning they will consider cloud-based delivery the preferred choice when implementing new services. Organizations are adopting cloud computing at this rapid pace to achieve speed, scale, and economic benefits. Azure is a cloud service that helps organizations deploy applications faster by providing a flexible platform for innovation offering global scale and enterprise-grade reliability. They can instantly provision applications and infrastructure, and save money with per-minute billing and built-in auto-scaling to meet changing business needs.

Azure can also help reduce the cost, complexity, and risk associated with security and compliance. A survey funded by Microsoft and conducted by ComScore demonstrates that while many organizations have initial concerns about moving to the cloud, a majority of cloud adopters achieve significant security benefits:

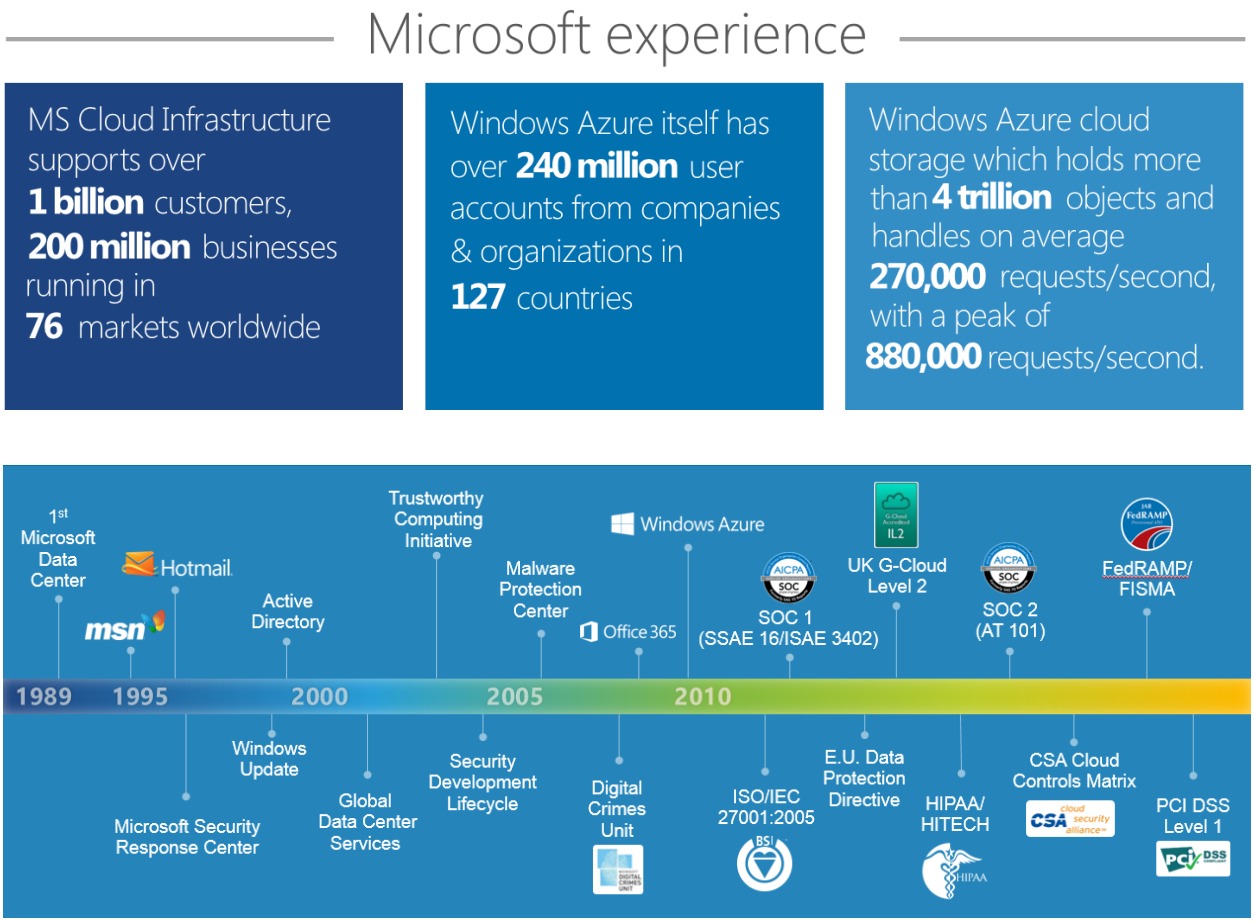
Few individual customer organizations can replicate the technology and operational processes that Microsoft uses to help safeguard its enterprise cloud services and comply with a wide range of international standards. When companies use Azure, they benefit from Microsoft's scale and experience running highly secure and compliant online services around the globe. Microsoft's expertise becomes the customer's expertise.

[1] (IDC CIO Agenda webinar)

Expertise, Partnership, and Transparency

Expertise through Experience

Microsoft has decades of unmatched experience building enterprise software and running some of the largest online services around the globe. Today, the Microsoft cloud infrastructure supports over 1 billion customers and 200 million businesses running in 76 markets worldwide. Microsoft has leveraged this expertise to create and implement industry-leading secure software development, operational management, and threat mitigation practices, helping it to deliver services that achieve higher levels of security, privacy, and compliance than most customers could achieve on their own.



Sharing Responsibility

Microsoft believes that security, privacy, and compliance for its enterprise cloud services are a shared responsibility. Microsoft helps reduce the security and compliance burden for customers by providing trustworthy enterprise cloud services, while also offering the security capabilities and flexibility customers need to use the services in accordance with their own standards.

Transparency and Independent Verification

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 meet compliance standards and demonstrating how compliance was achieved, Microsoft makes it easier for customers to attain compliance for the infrastructure and applications they run in Azure.

How Azure Helps Keep Data Safe

Design and Operational Excellence

Azure security, privacy, and compliance begin with a trustworthy technology foundation. Microsoft creates, implements, and continuously improves security-aware software development, operational, and threat mitigation practices. This helps customers reduce the time and money they spend on implementing and maintaining the security of their computing platform.

"With Azure, we don't have to worry about data center infrastructure. Microsoft takes care of … maintenance tasks so we can focus on what we do best—designing innovative mailing solutions."

– Paul Aronson, Director of Engineering, Pitney Bowes (USA)

Security Centers of Excellence. Microsoft engages in industry-leading security efforts through the creation of centers of excellence, including the Microsoft Digital Crimes Unit, Microsoft Cybercrime Center, and Microsoft Malware Protection Center.

Designing for security from the ground up. Azure development adheres to the Security Development Lifecycle (SDL). The SDL became central to Microsoft's development practices a decade ago and is shared freely with the industry and customers. It embeds security requirements into systems and software through the planning, design, development, and deployment phases.

Keeping operations safe. Azure adheres to a rigorous set of security controls that govern operations and support. The Azure team works with other entities within Microsoft such as Office 365 and the Microsoft Operational Security Assurance (OSA) group to identify risks and share information, supporting continuous improvement in operational controls. This increases the ability to

prevent, detect, contain, and respond to operational security threats specific to Azure and company-wide.

Assume breach. One key operational best practice that Microsoft uses to harden its cloud services is known as the "assume breach" strategy. A dedicated "red team" of software security experts simulates real-world attacks at the network, platform, and application layers, testing Azure's ability to detect, protect against, and recover from breaches. By constantly challenging the security capabilities of the service, Microsoft can stay ahead of emerging threats.

Incident response. Azure has a global, 24x7 incident response service that works to mitigate the effects of attacks and malicious activity. The incident response team follows established procedures for incident management, communication, and recovery, and uses discoverable and predictable interfaces internally and to customers.

Infrastructure Protection

Azure infrastructure includes hardware, software, administrative and operations staff, and physical data centers. Azure addresses security risks across its infrastructure with continuous intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools that help identify and mitigate threats. With Azure, customers can reduce the need to invest in these capabilities on their own and benefit from economies of scale in Microsoft datacenter infrastructure.

24-hour monitored physical security. Microsoft datacenters are physically constructed, managed, and monitored 24 hours a day to shelter data and services from unauthorized access as well as environmental threats.

Monitoring and logging. Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Azure environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

Patch management. Security patches help protect systems from known vulnerabilities. Integrated deployment systems manage the distribution and installation of security updates for the Azure service. Customers can apply similar update management processes for virtual machines (VMs) deployed on Azure.

Anti-Virus/Anti-Malware protection. Microsoft Antimalware is built-in to 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. Customers can also run antimalware solutions from partners on their VMs. For added assurance, VMs can be routinely reimaged to clean out intrusions that may have gone undetected.

Intrusion detection/Distributed Denial of Service (DDoS) Defense. Azure uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits to protect against DDoS attacks. The Azure DDoS defense system is designed to withstand attacks from outside the system as well as attacks staged by other customers.

Penetration testing. Microsoft conducts regular penetration testing to improve Azure security controls and processes. Customers can carry out authorized penetration testing on their applications hosted in Azure.

Network Protection

Azure networking provides the infrastructure necessary to securely connect VMs to one another and to connect on-premises data centers with Azure VMs. Azure blocks unauthorized traffic to and within Microsoft data centers using a variety of technologies such as firewalls, partitioned Local Area Networks, and physical separation of back-end servers from public-facing interfaces.

Network isolation. Network isolation prevents unwanted tenant-to-tenant communications, and access controls block unauthorized users from the network. Virtual machines do not receive inbound traffic from the Internet unless customers configure them to do so.

Virtual networking. A customer can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other using private IP addresses. Each virtual network is isolated from other virtual networks.

Encrypting communications. Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Azure regions, and from Azure to on-premises data centers. Encryption can be configured to protect administrator access to virtual machines through remote desktop sessions and remote Windows PowerShell. Access to the Azure Management Portal is encrypted by default using HTTPS.

Using Express Route. Customers can use an optional Express Route private fiber link into Azure data centers to keep their traffic off the Internet.

Identity and Access

Azure enables customers to control access to their environments, data and applications. Microsoft offers comprehensive and federated identity and access management solutions for customers to use across Azure and other services such as Office 365, helping them simplify the management of multiple environments and control user access across applications.

"We are delivering greater value to our customers because we are able to cut down on costs, complexity, and development time by taking advantage of Azure Active Directory."

– Rick Hinton, Vice President Products and Solutions, at Portal Solutions

Enterprise cloud directory. Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory services, advanced identity governance, security, and application access management. Azure Active Directory makes it easy for developers to build policy-based identity management into their applications. Azure Active Directory Premium includes additional features to meet the advanced identity and access needs of enterprise organizations.

Access monitoring and logging: 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. Customers can turn on additional access monitoring functionality in Azure and use third-party monitoring tools to detect additional threats. Customers can request reports from Microsoft that provide information about user access to their environments.

Strong authentication. 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, to secure employee, customer, and partner access. Azure Multi-Factor Authentication can be used for both on-premises and cloud applications.

Role-based access control. Multiple tools in Azure support authorization based on their role, simplifying access control across defined groups of users.

Data Protection

Both technological safeguards, such as encrypted communications, and operation processes help keep Customer Data secure. Customers have the flexibility to implement additional encryption and manage their own keys.

Data in transit. Azure uses industry-standard transport protocols such as SSL and TLS between user devices and Microsoft data centers, and within data centers themselves. With virtual networks, customers can use industry standard IPsec protocol to encrypt traffic between their corporate VPN gateway and Azure. Customers can enable encryption for traffic between their own VMs and end users.

Data at rest. Customers are responsible for ensuring that data stored in Azure is encrypted in accordance with their standards. Azure offers a wide range of encryption capabilities up to AES-256, giving customers the flexibility to choose the solution that best meets their needs. Options include .NET cryptographic services, Windows Server public key infrastructure (PKI) components, Microsoft StorSimple cloud-integrated storage, Active Directory Rights Management Services (AD RMS), and BitLocker for data import/export scenarios.

"With Azure, we could quickly insert a standard secure socket layer (SSL) to exchange financial data with banks. Privacy was also a big concern, because customers want their commercial data secured. Again, Azure was attractive because it has built-in capabilities for compliance with a wide range of regulations and privacy mandates."

– Natthaseth Sirinanthanon
General Manager, Semantic Touch

Data segregation. Azure is a multi-tenant service, meaning that multiple customers' deployments and virtual machines are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.

Data destruction. When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before reuse, as well physical destruction of decommissioned hardware.

Privacy

Microsoft recognizes that cloud services raise unique privacy challenges for businesses. That is why it implements strong privacy protections in Azure services and makes commitments to safeguard the privacy of customer data. In addition, Microsoft provides customers with visibility into where their data resides and who has access to it.

Privacy by Design. With Microsoft, customers can expect Privacy by Design, a policy that guides how Microsoft builds products and services, how services are operated, and how internal teams are organized.

"Our vision is to be the national leader in patient-centered e-healthcare. Using Azure as our delivery system provides us with a level of trust and reliability that makes this possible."

– Alan Rogam, MD
Founder and Chief Executive Officer,
Stat Health Services

Contractual commitments. 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. Microsoft 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 transfers of personal data.

Control over data location. For many customers, knowing and controlling the location of their data can be an important element of data privacy compliance and governance. Azure customers can specify the geographic areas where their customer data is stored. Data may be replicated within a geographic area for redundancy, but will not be transmitted outside it. For more information, including exceptions to this policy, see the Azure Trust Center.

Restricted data access and use. Access to customer data by Microsoft personnel is restricted. Customer Data is only accessed when necessary to support the customer's use of Azure. This may include troubleshooting aimed at preventing, detecting or repairing problems affecting the operation of Azure and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). When granted, access is carefully controlled and logged. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed.

No use for advertising. Azure does not share Customer Data with its advertiser-supported services, nor is customer data mined for advertising.

Compliance

Microsoft maintains a team of security, privacy, and compliance experts who help Azure meets its own compliance obligations. The compliance team also represents the "customer voice," working with Microsoft engineering and operations teams as well as external regulatory bodies to help ensure customers' needs are met.

Microsoft invests heavily in the development of robust and innovative compliance processes. The Microsoft compliance framework for online services maps controls to multiple regulatory standards. This enables Microsoft to design and build services using a common set of controls, streamlining compliance across a range of regulations today and as they evolve.

Microsoft compliance processes also make it easier for customers to achieve compliance across multiple services and meet their changing needs efficiently. Together, security-enhanced technology and effective compliance processes enable Microsoft to maintain and expand a rich set of third-party certifications. These help customers demonstrate compliance readiness to customers, auditors, and regulators. As part of its commitment to transparency, Microsoft shares third-party verification results with its customers.

Azure is certified for **ISO 27001**, a broad international information security standard, and undergoes annual audits for ISO compliance. Azure has also been audited against the Service Organization Control (SOC) reporting framework for **SOC 1 Type 2**, attesting to the design and operating effectiveness of its controls. In addition, Azure has been audited for **SOC 2 Type 2**, which includes a further examination of Azure controls related to security, availability, and confidentiality. Azure undergoes annual SOC audits.

Azure has also obtained many industry-specific certifications, including:

- **Payment Card Industry (PCI) Data Security Standard (DSS):** Azure has been validated for PCI-DSS compliance by an independent Qualified Security Assessor (QSA). Designed to help prevent fraud through increased controls involving credit card data, certification is required for all organizations that store, process, or transmit credit card information. Customers can reduce the complexity of their PCI-DSS certification by using compliant services on Azure.

- **United States FedRAMP:** Azure has received Provisional Authorization to Operate from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB), having undergone the assessments necessary to verify that it meets FedRAMP security standards.
- In the **United Kingdom**, Azure has been awarded **Impact Level 2 (IL2)** accreditation, further enhancing Microsoft and its partner offerings on the current G-Cloud procurement Framework and CloudStore.
- **Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH):** To help customers comply with HIPAA and HITECH Act security and privacy provisions, Microsoft offers a HIPAA Business Associate Agreement (BAA) to healthcare entities with access to Protected Health Information (PHI).

For more details on the scope of compliance certifications, visit the Azure Trust Center. It is important to note that Microsoft generally treats verifications as a baseline and frequently goes far beyond them in its commitment to deliver trustworthy, compliance-ready services.

Cloud Security Alliance. Microsoft participates in industry-wide transparency initiatives, especially through its association with the Cloud Security Alliance (CSA). An independent industry organization, the CSA has developed a controls framework called the Cloud Controls Matrix (CCM). The CCM provides organizations with a standards-based, industry-vetted, framework that incorporates cloud services. Microsoft publishes information about how it addresses the CSA CCM in the publically accessible CSA Security, Trust & Assurance Registry (STAR).

Cloud Risk Assessment Tools, Microsoft gives customers free tools that help them achieve compliance on their own terms such as the Cloud Risk Decision Framework and Cloud Risk Assessment models, both of which are based on the globally-recognized Enterprise Risk Management standard ISO 31000. Organizations wishing to evaluate their IT security state, evaluate the benefits of cloud computing, and plan for adoption can use the Cloud Security Readiness Tool. Using the answers to a few short questions, it generates a report tailored to the needs of the organization.

For more information, read the white paper "The Microsoft Approach to Cloud Transparency."

Transform Security and Compliance with Azure

Microsoft provides a deep, tenured commitment to security, privacy, and compliance, which helps Azure customers maximize the security and compliance benefits of the cloud. Azure delivers a trusted platform that enables companies to move to the cloud more quickly while leveraging Microsoft expertise to reduce risk. To learn more about Azure security and compliance, visit the Azure Trust Center. Or, experience it yourself with a free trial.

Resources

- **Azure Website** | http://azure.microsoft.com/
- **http://azure.microsoft.com/en-us/support/trust-center/** | http://azure.microsoft.com/en-us/support/trust-center/
- **Azure Security: Technical Insights** | http://go.microsoft.com/?linkid=9740388
- **Security Best Practices for Developing Azure Solutions: Technical Insights** | http://go.microsoft.com/fwlink/?LinkID=392589
- **Azure Networking White Paper** | http://download.microsoft.com/download/4/3/9/43902EC9-410E-4875-8800-0788BE146A3D/Windows%20Azure%20Network%20Security%20Whitepaper%20-%20FINAL.docx