The Microsoft approach to cloud transparency

Using the Cloud Security Alliance's Security, Trust & Assurance Registry (STAR)

The Microsoft approach to cloud transparency

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Authors

Frank Simorjay
Microsoft Trustworthy Computing

Ariel Silverstone
Concise Consulting

Aaron Weller
Concise Consulting

Contributors

Kellie Ann Chainier
Microsoft Public Sector

Stephanie Dart
Microsoft Dynamics CRM

Mark Estberg
Global Foundation Services

John Howie
Global Foundation Services

Marc Lauricella
Microsoft Trustworthy Computing

Kathy Phillips
Microsoft Legal and Corporate Affairs

Tim Rains
Microsoft Trustworthy Computing

Sian Suthers
Microsoft Trustworthy Computing

Stevan Vidich
Windows Azure Marketing

Steve Wacker
Wadeware LLC

Table of contents

Executive summary

The shift to cloud computing represents a significant opportunity to change the way that businesses operate. Similar to the concept of *outsourcing,* the combination of the technologies and processes that comprise today's definition of cloud computing represent a new way to view and use information technology and enhance the value of IT organizations.

This evolution of computing represents a tremendous opportunity for many organizations, because they can reduce or eliminate the need to manage the server-based technologies that underlie their business processes. In addition to changing processes and focus, this shift provides ways to reduce costs, to be more agile in adjusting to rapidly changing business needs, and to deploy and track resources in a more efficient manner.

This paper provides an overview of various risk, governance, and information security frameworks and standards. It also introduces the cloud-specific framework of the Cloud Security Alliance (CSA), known as the Security, Trust & Assurance Registry (STAR).

STAR is a good resource for organizations that seek an unbiased information source to help them evaluate cloud providers and maximize the benefits of cloud service. Microsoft's commitment to transparency is apparent in its adoption of STAR controls for security, privacy, compliance, and risk management and also in its replies to STAR control requirement statements, some of which are included later in this paper.

Introduction

Cloud computing is a way of treating computing as a utility service. That is, computer processing, storage, and bandwidth are managed as commodities by providers, similar to electricity or water. This approach represents a logical evolution of computing for many organizations; taking advantage of cloud computing means that they reduce or eliminate the need to manage the server-based technologies that underlie their business processes, and can focus on their core business activities.

In addition to providing organizations with the ability to focus on their core business objectives, cloud computing can help them reduce information technology and capital costs, which can provide better results to stakeholders. Also, cloud computing helps IT organizations support new business needs of their existing customer base by providing rapid deployment and resource utilization tracking. This capability directly contributes to business *agility,* the ability to adapt to new conditions and quickly bring new solutions to market.

Cloud computing provides an opportunity for organizations to take advantage of the rapid evolution of technology and benefit from related security, speed, scalability, and flexibility opportunities without being burdened by on-premises solutions. Today, organizations are frequently challenged to reduce their IT costs but are required to be agile and responsive to market needs. The cloud computing model allows them to pay only for the services they need.

Capital outlay can be reduced significantly, which allows them to prioritize resources on business objectives.

The inherent agility in cloud computing also provides an additional benefit: scalability. As business needs grow and features or sets of data are added, cloud computing allows simple and fast *scaling* of the environment. Should the computing environment's capacity need to be reduced, for example after a seasonal peak, it can be easily facilitated without the negative effects that typically accompany the sudden idling of a significant capital investment.

The opportunity offered by cloud computing requires balancing the benefits of moving data, processing, and capacities to the cloud with the implications of data security, privacy, reliability, and regulatory requirements. Since the launch of MSN® in 1994, Microsoft has been building and running online services. Microsoft enables organizations to adopt cloud computing rapidly via its cloud services such as Windows Azure™, Office 365, and Microsoft Dynamics® CRM and take a business-leading approach to security, privacy, and reliability.

Microsoft cloud services are hosted in Microsoft data centers around the world, and are designed to offer the performance, scalability, security, and service levels that business customers expect. Microsoft has applied state-of-the-art technology and processes to maintain consistent and reliable access, security, and privacy for every user. These Microsoft cloud solutions have capabilities that facilitate compliance with a wide range of global regulations and privacy mandates.

In this paper, Microsoft provides an overview of various risk, governance, and information security frameworks and introduces the cloud-specific framework developed by the Cloud Security Alliance (CSA), called the Security, Trust & Assurance Registry (STAR). The paper also discusses STAR's roots and evolution, and examines how Microsoft cloud products fulfill the security, privacy, compliance, and risk management requirements that are defined in STAR.

This white paper provides information about how Microsoft services such as Windows Azure, Office 365, and Microsoft Dynamics CRM align with STAR guidelines for security, privacy, compliance, and risk management controls.When engaging customers, Microsoft provides documentation that specifies Microsoft-shared responsibilities with regard to applications and data that customers entrust to them; such documentation is essential for organizations that have regulatory and/or compliance obligations. As with any use of a third-party service, the customer that uses the service is ultimately accountable for determining whether the service meets their needs and obligations.

With regard to Windows Azure, this white paper addresses Windows Azure core services: Cloud Services (Web and Worker roles, formerly under Compute), Storage (Tables, Blobs, Queues), and Networking (Traffic Manager and Windows Azure Connect). It does not provide detailed information about other Windows Azure features, such as Windows Azure SQL Database, Service Bus, Marketplace, and Caching.. For more information about Windows Azure, see the "Additional reading" section later in this paper. Office 365 and Microsoft Dynamics CRM Online services run on a cloud infrastructure provided by Microsoft and are accessible from various client devices.

This white paper assumes that readers are familiar with Windows Azure basic concepts; therefore, they are not explained within the paper. Links to reading materials that describe these core concepts can be found at "White Papers on Windows Azure" on Technet.

Cloud assurance challenges

Having a good grasp of risk management is important in today's information security and privacy landscape.

When working with cloud computing providers such as Windows Azure and cloud-provided services such as Office 365 and Microsoft Dynamics CRM, it is important to understand that risk assessments need to consider the dynamic nature of cloud computing.

An organization needs to consider performing a full-scope risk assessment that looks at several criteria whenever a new initiative is underway. Cloud computing is no different. Some of the more prominent criteria that typically interest organizations that are considering cloud computing deployments are discussed in the following sections.

Security

There are many security dimensions to consider in cloud computing scenarios.

Layers

When evaluating controls in cloud computing, it is important to consider the entire services stack of the cloud service provider. Many different organizations may be involved in providing infrastructure and application services, which increases the risk of misalignment. A disruption of any one layer in the cloud stack, or in the customer-defined last mile of connectivity, could compromise the delivery of the cloud service and have negative impacts. As a result, customers should evaluate how their service provider operates and understand the underlying infrastructure and platforms of the service as well as the actual applications.

Secure data destruction or erasure

Many organizations have policies that require data to be deleted when it is no longer needed, or after a fixed interval. At times, these policies mandate that data deletion be attested to, which may take the form of a statement that the data has been destroyed in a manner that prevents its reconstruction.

Many cloud providers cannot easily attest to such deletion, partially because of the way cloud data is rapidly replicated and relocated on many disk drives, servers, and data centers. Although the assumption may be that such data is overwritten in its "original" or prior location, the possibility frequently exists that a determined forensic process (or attack) could retrieve such data.

Data loss

Cloud computing in its current multi-tenant form is relatively new, and many deploying organizations are concerned with the maturity of the tools used by providers to host and manage their data.

Microsoft stands out from newer entrants to the market because of its experience in related technology platforms (such as Hotmail®, MSN®, and others), as many as twenty years in some cases.

Beyond the typical risk of data loss on disk drives, the existence of additional tools such as hypervisors, virtual machine managers, new operating and storage environments, and rapidly deployed applications introduce additional stability and redundancy factors that must be included in data loss considerations.

Privacy

As part of the security risk assessment, a privacy review needs to be considered to ascertain potential risks to the data and operations in the cloud. Today, the notion of privacy goes beyond the traditional description of customer data and extends into *organizational* privacy, which includes most intellectual property constraints; that is, the know-how, know-why, and know-when of organizations. As more and more organizations become knowledge-based, the intellectual property values that they generate increase. In fact, intellectual property value is often a significant part of an organization's value.

Confidentiality and integrity

Similarly, concerns about *confidentiality* (who can see the data) and *integrity* (who can modify the data) are important to include in any evaluation. Generally, the more access points to the data, the more complicated the risk profile creation process. Although many regulatory frameworks focus on confidentiality, others such as Sarbanes-Oxley focus almost exclusively on the integrity of data that is used to produce report financial statements.

Reliability

In many cloud computing environments, the data flow that moves information into and out of the cloud must be considered. Sometimes multiple carriers are involved, and oftentimes access beyond the carrier must be evaluated. For example, a failure at a communications service provider can cause delay and affect the reliability of cloud-based data and services. Any additional service provider must be evaluated and assessed for risk.

Auditing, assurance, and attestation

Many organizations are experienced in traditional application and data deployment activities, such as auditing and assessments. In a cloud deployment, the need for some of these activities becomes even more acute at the same time that the activities themselves become more complex.

Embedded in the cloud concept, and especially in public cloud deployment, is a lack of physical control by the organization that owns the data. Physical controls must be considered to protect the disk drives, the systems, and even the data centers in which data resides. Such considerations also apply to software environments in which cloud services components are deployed.

In addition, obtaining permissions for the purpose of satisfying requirements for resiliency testing, penetration testing, and regular vulnerability scanning can be a challenge in cloud deployments.

It can also be a challenge to address and satisfy requirements for independent validation of controls. Cloud providers are typically reluctant to approve many types of testing in a shared infrastructure because of the impact that testing could have on other customers.

> Frequently, an organization intending to engage in cloud deployment does not know how to evaluate risks or how to choose a cloud provider that mitigates risks.

For certain regulatory frameworks, auditing is a requirement. Frequently, cloud customers are faced with challenges that threaten or appear to deny the many benefits of cloud adoption and deployment.

The benefits of standardized frameworks

Generally, core competencies of organizations that adopt cloud computing do not include the deployment and management of cloud computing technologies. Because of the potential common and cloud-specific risks, organizations frequently rely on outside consulting firms and cloud providers' lengthy RFP responses to evaluate risk for their specific cloud deployment needs.

Those responses must be evaluated by experienced cloud professionals, in addition to internal risk experts, to ascertain the true risk to the organization. This risk assessment should include a determination of the risk that derives from adopting these technologies and how to best mitigate that risk.

The cloud deployment partner selection exercise frequently takes place in a climate of intense business pressure to reduce costs and to increase flexibility. In such a climate, a drawn-out risk management process may be seen as an inhibitor, rather than an enabler, of business goals.

Best practices

Some of the unease and complexity involved in selecting a cloud provider can be alleviated by using a common controls framework. Such a framework should consider not only best practices in information security, but also include a true understanding and evaluation of cloud-specific deployment considerations and risks. In addition, such a framework should address much of the cost involved in the evaluation of alternate solutions and help to significantly manage risk that must otherwise be considered.

> In using a well thought-out controls framework, organizations can avoid most of the costs related to engaging outside expertise for selecting an appropriate cloud provider, and rely instead on combined efforts that represent years of expertise in the field.

Complexity

A cloud-specific controls framework such as the Cloud Controls Matrix (CCM) reduces the risk of an organization failing to consider important factors when selecting a cloud provider. The risk is further mitigated by relying on the cumulative knowledge of industry experts who created the framework, and taking advantage of the efforts of many organizations, groups, and experts in a thoughtfully laid-out form. In addition, an effective industry framework will be regularly updated to take account of changes in maturing technologies, based on the experiences of experts who have reviewed many different approaches.

Comparison

For organizations that do not have detailed knowledge about the different ways that cloud providers can develop or configure their offerings, reviewing a fully developed framework can provide insight into how to compare similar offerings and distinguish between providers. A framework can also help determine whether a specific service offering meets or exceeds compliance requirements and/or relevant standards.

Audit and knowledge base

Using an industry-accepted framework provides a means to review documentation about why and how decisions were made and to know which factors were given more weight and why. Understanding how a decision was made can provide a basis of knowledge for decision making in future efforts, especially when personnel changes cause the people who made the original decision to no longer be available.

Security standards evolution

Deciding which standard and framework to apply when selecting a cloud computing provider used to require organizations to choose from frameworks written in a pre-cloud computing environment. Commonly used risk, control, and information security frameworks include the 27000 family of standards published by the International Organization for Standardization/International Electrotechnical Committee (ISO/IEC); COBIT, a framework for the governance and management of enterprise IT by Information Systems Audit and Control Association (ISACA); the SP800 series of standards by the U.S. National Institute of Standards and Technology (NIST), and a few others.

The International Organization for Standardization/International Electrotechnical Committee (ISO/IEC) 27000 family of standards

The ISO family of standards includes some of the world's best-known information security reference frameworks. British Standard 7799 Part 1 first became internationalized as "The Code of Practice for Information Security Management" in 2000 and was referred to as ISO/IEC 17799. In 2007, this designation was changed to ISO 27002. The current version, ISO 27002:2005, is generally accepted today as the guide for implementation of information security management frameworks.

ISO/IEC 27001 came from British Standard 7799 Part 2, and defines how to implement, monitor, maintain, and continually improve an information security management system (ISMS). It uses the ISO/IEC standard Plan-Do-Check-Act framework.

Organizations can be certified against the ISO/IEC 27001 standard, as Microsoft has done with Windows Azure (core services) and several other Microsoft online services (identified later in this section), which has led to ISO/IEC 27001 adoption by organizations looking to validate their information security efforts with customers, regulators, or other external stakeholders.

Today, the 27000 standards family has grown to include the following standards:

- ISO/IEC 2700**0**:2009, Information security management systems — Overview and vocabulary
- ISO/IEC 2700**1**:2005, Information security management systems — Requirements
- ISO/IEC 2700**2**:2005, Code of practice for information security management
- ISO/IEC 2700**3**, Information security management system implementation guidance
- ISO/IEC 2700**4**, Information security management — Measurement
- ISO/IEC 2700**5**:2008, Information security risk management
- ISO/IEC 2700**6**:2007, Requirements for bodies providing audit and certification

The ISO/IEC 27000 family of standards, and in particular ISO/IEC 27002, constitutes the generally accepted standards for today's information security management.

- ISO/IEC 2700**7**:2011, Guidelines for information security management systems auditing
- ISO/IEC 2703**1**:2011, Guidelines for information and communications technology readiness for business continuity

Windows Azure, Microsoft Dynamics CRM, Office 365, and the underlying Global Foundation Services (GFS) infrastructure layer employ security frameworks based on the ISO/IEC 27001:2005 standard.

Windows Azure core services (Cloud Services, Storage, and Networking), Microsoft Dynamics CRM, and Office 365 are ISO 27001-certified. In addition, the physical GFS infrastructure on which all of Windows Azure runs (except CDN) and on which both Office 365 and Microsoft Dynamics CRM run, is ISO 27001-certified.

The Microsoft security framework, based on ISO/IEC 27001, enables customers to evaluate how Microsoft meets or exceeds the security standards and implementation guidelines. In addition, Windows Azure and the GFS infrastructure undergo annual Statement on Auditing Standards No. 70 (SAS 70 Type II or its successor, SSAE16 and additionally ISAE 3402) audits.

There is no ISO/IEC 27002 certification process. However, the standard provides a suggested set of suitable controls for an Information Security Management System, which is documented in ISO/IEC 27001 Annex A.

The Information Security Policy, which applies to Microsoft cloud offerings, also aligns with ISO/IEC 27002 and is augmented with requirements specific to Microsoft cloud offerings.

Links to the public copies of the Windows Azure, Microsoft Dynamics CRM, Office 365, Global Foundation Services, and FOPE ISO certifications are available in the "Additional reading" section later in this paper.

COBIT

The Control Objectives for Information and related Technology (COBIT) framework is a well thought-out and generally accepted standard that was published to help organizations evaluate information technology-related risk.

First published in 1996 and currently in its fifth revision (published in 2012), COBIT is published by the *IT Governance Institut*e, which is affiliated with the Information Systems Audit and Control Association (ISACA). Although the previous version (4.1, published in 2007) was organized by using 34 high-level processes and 215 detailed control objectives, the new version is different. For COBIT 5, ISACA chose to partition the document into 37 high-level processes and 17 *goals*. COBIT is designed to bridge management and control gaps between technical and business risks.

For more information about COBIT, see the "Additional reading" section later in this paper.

> COBIT is a very useful tool to help correlate disparate standards such as the Information Technology Infrastructure Library (ITIL), Capability Maturity Model Integration (CMMi), and ISO 27002.

NIST Special Publication (SP) 800 series

The U.S. National Institute of Standards and Technology (NIST) publishes various standards for use by U.S. government agencies and departments. Most notable among these standards is the SP800 series, which focuses on security and privacy. NIST was the originator of the globally accepted working definition of cloud computing, which is now published as Draft SP800-145. This draft publication has been submitted to the ISO/IEC standards body for inclusion in a forthcoming international standard.

Also of note in the SP800 series is SP800-53, which defines the security controls that must be implemented in computing solutions to meet the requirements of the Federal Information Security and Management Act (FISMA). The controls are also found in the Federal Risk and Authorization Management Program (FedRAMP), which is a U.S. government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Microsoft has achieved FISMA Moderate Authorization to Operate (ATO) for GFS and Office 365.

Introducing STAR

With the emergence of cloud computing and the increased market understanding of its tremendous potential to help organizations create, manage, and maintain tools to achieve growth, it has become clear that existing standards as discussed in the previous section may no longer be effective to address concerns about the rapid implementation and novel business uses of this powerful technology.

The Cloud Security Alliance (CSA) and STAR

The Cloud Security Alliance (CSA) is a not-for-profit organization that promotes the use of best practices for security assurance within cloud computing. To reduce much of the effort, ambiguity, and costs of getting the most relevant questions and information on cloud providers' security and privacy practices, the CSA has published and maintains the *Security, Trust & Assurance Registry (STAR)*.

> Per the Cloud Security Alliance at *https://cloudsecurityalliance.org/star/*
> STAR is a "free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with."

STAR domains

STAR uses the following 13 domains to address cloud computing security

- Cloud Computing Architectural Framework
- Governance and Enterprise Risk Management
- Legal and Electronic Discovery
- Compliance and Audit
- Information Lifecycle Management
- Portability and Interoperability
- Traditional Security, Business Continuity, and Disaster Recovery
- Data Center Operations
- Incident Response, Notification, and Remediation
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization

Cloud Controls Matrix (CCM)

STAR uses the Cloud Controls Matrix (CCM) to provide a controls framework for understanding security, privacy, and reliability concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. This paper uses CCM version 1.2 currently the released version, which comprises a list of 100 questions. The CSA CCM provides organizations with a framework that has the needed structure, detail, and clarity with regard to information security, tailored to the service providers in the cloud industry.

Providers may choose to submit a report that documents their compliance with the CCM, and such reports are published by STAR.

> Microsoft has published an overview of its capabilities in meeting the CCM requirements. The goal of this STAR-registered overview is to empower customers with information to evaluate Microsoft offerings.

Consumers of cloud services can then use the data contained in STAR to evaluate providers and to identify questions that would be prudent to have providers answer before moving to adopt cloud services. (STAR is a self-assessment-based process by the cloud providers, and the CSA does not audit or guarantee the responses that are provided. Microsoft has chosen to not only address each of the 100 questions in the STAR CCM but also to align the domains to the ISO 27001 certifications received by various Microsoft services to provide an additional layer of comfort to consumers of cloud services.)

Aligning to STAR

When mitigating risk while deploying a cloud solution, an organization must consider the cloud-specific risks described in the preceding “Cloud assurance challenges” section as well as organizational goals. Common as well as cloud-specific risks must be weighed and evaluated carefully to assure the best results for the organization.

One *best practice* is to proceed with the selection of a cloud provider as described earlier, by using a common framework. This approach will help mitigate risk but also help avoid the cost of engaging outside expertise and a costly independent review process, relying instead on combined efforts that represent years of expertise in the field.

> Using STAR, an organization can compare various cloud offerings, select criteria important to the organization, and document how and why a specific solution was selected. This approach helps mature future selection efforts and adds to the organization’s knowledge base.

Organizations can use the control criteria in the CCM to help mitigate the risk of missing important evaluation criteria. STAR also allows organizations to use a fully developed framework to carefully compare similar offerings. In addition, it can provide a way to measure and quantify weighting factors for related criteria.

Specific examples of Microsoft adoption of STAR controls

To provide some specific examples of how the STAR framework helps both an initial selection process and ongoing due diligence, Microsoft has selected some specific examples of STAR controls and the corresponding Microsoft responses.

Full STAR submissions downloads

Microsoft Dynamics CRM Online	Summited April 05, 2012
Microsoft Office 365	Submitted December 02, 2011
Microsoft Windows Azure	Submitted March 30,2012

In the following examples, an organization can see how they can save time and money by using the CCM framework to obtain standard answers from cloud providers instead of developing their own lists of questions. For example, an organization can select the questions that are most relevant and compare the answers of Microsoft and other providers to help decide which service to select. The examples apply to Windows Azure, Office 365, and Microsoft Dynamics CRM.

CO-01 Compliance - Audit planning

“Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.”

Microsoft’s reply:

“Microsoft’s goals are to operate Microsoft‘s services with security as a key principle, and to give the customer accurate assurances about Microsoft‘s security. Microsoft has implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.

Each year, Microsoft undergoes third-party audits by internationally recognized auditors to validate that Microsoft has independent attestation of compliance with Microsoft‘s policies and procedures for security, privacy, continuity, and compliance

ISO 27001 certifications for Microsoft Dynamics CRM, Windows Azure, Office 365, and Global Foundation Services (which runs the physical infrastructure) can be found on the website of Microsoft’s external ISO auditor, the BSI Group. Additional audit information is available under NDA upon request by prospective customers.

Windows Azure,Office 365, and Microsoft Dynamics CRM Online independent audit reports and certifications are shared with customers in lieu of allowing individual customer audits. These certifications and attestations accurately represent how Microsoft obtains and meets Microsoft's security and compliance objectives and serve as a practical mechanism to validate Microsoft's promises for all customers.

For security and operational reasons, Windows Azure, Office 365, and Microsoft Dynamics CRM do not allow Microsoft customers to perform their own audits.

Customers *are* allowed to perform non-invasive penetration testing of their own application on the Windows Azure platform with prior approval."

"Monitor and review the Information Security Management System (ISMS)" is covered under the ISO 27001 standards, specifically addressed in Clause 4.2.3. For more information, review of the publicly available ISO standards we are certified against is suggested."

DG-05 Data Governance – Secure Disposal

"How does the service provider comply with the need for 'Policies and procedures shall be established and mechanisms implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.'"

Microsoft's reply:

"Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that can't be wiped, we use a destruction process that destroys it (such as shredding) and renders the recovery of information impossible (for example, disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained.

Microsoft Dynamics CRM Online uses approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle.

All Windows Azure services utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle.

Microsoft Office 365 utilizes approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle."

"Secure disposal or re-use of equipment and disposal of media" is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 9.2.6 and 10.7.2. For more information, we suggest a review of the publicly available ISO standards for which we are certified."

FS-03 Facility Security - Controlled Access Points

"Physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) shall be implemented to safeguard sensitive data and information systems."

Microsoft’s reply:

“Data center buildings are nondescript and do not advertise that Microsoft Data Center hosting services are provided at the location. Access to the data center facilities is restricted. The main interior or reception areas have electronic card access control devices on the perimeter door(s), which restrict access to the interior facilities. Rooms within the Microsoft Data Center that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are either restricted through various security mechanisms such as electronic card access control, keyed lock, antitailgating and/or biometric devices.

Additional physical barriers, such as “locked cabinets” or locked cages erected internal to facility perimeters, may be in place as required for certain assets according to Policy and/or by business requirement.”

“Physical security perimeter and environmental security” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9. For more information review of the publicly available ISO standards Microsoft is certified against is suggested.“

SA-12 Security Architecture – Clock Synchronization

“An external accurate, externally agreed upon, time source shall be used to synchronize the system clocks of all relevant information processing systems within the organization or explicitly defined security domain to facilitate tracing and reconstitution of activity timelines. Note: specific legal jurisdictions and orbital storage and relay platforms (US GPS & EU Galileo Satellite Network) may mandate a reference clock that differs in synchronization with the organizations domicile time reference, in this event the jurisdiction or platform is treated as an explicitly defined security domain.”

Microsoft’s reply:

“In order to both increase the security of Microsoft Dynamics CRM Online, Windows Azure, and Office 365 and to provide accurate reporting detail in event logging and monitoring processes and records, Microsoft Dynamics CRM Online, Windows Azure, and Office 365 use consistent clock setting standards (such as PST, GMT, UTC). When possible, Microsoft Dynamics CRM Online, Windows Azure, and Office 365 server clocks are synchronized through the Network Time Protocol which hosts a central time source for standardization and reference, in order to maintain accurate time throughout the Microsoft Dynamics CRM Online, Windows Azure, and Office 365 environments.”

“Clock synchronization” is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 10.10.6. For more information review of the publicly available ISO standards we are certified against is suggested.”

Summary

The decision about how to move forward with cloud deployment is an important one. As organizations see the benefits of cloud computing in rapid deployment and provisioning, up or down-scaling, and cost reduction, they find cloud migration a desirable approach to service delivery.

However, such migration and deployment of new services are sometimes slowed or prevented by the need to thoroughly research (or assess) the risk involved and mitigate such risk. In the process of implementing cloud computing, much of the risk is seen as new, or even exotic, when compared to existing, day-to-day, operational risk.

Some of the unease and complexity involved in selecting a cloud provider can be alleviated by using a common controls framework. Such a framework should be based upon industry best practices and a true understanding and evaluation of cloud-specific deployment considerations and risks. Such a framework should also help alleviate much of much of the cost involved in the evaluation of alternate solutions, and help to significantly manage risks that are inherent in the deployment of any new technology.

The Security, Trust and Assurance Registry, created by the Cloud Security Alliance (CSA), is such a framework.

The CSA publishes and maintains STAR, which was created to reduce much of the effort, ambiguity, and costs of getting the right information on cloud providers' security and privacy practices. STAR uses the Cloud Controls Matrix (CCM) to provide a detailed understanding of security and privacy concepts and principles that are aligned with Cloud Security Alliance guidance.

> The CSA CCM provides organizations with a framework that has the needed structure, detail, and clarity with regard to information security, tailored to the cloud computing services industry.

To help organizations deploy cloud computing solutions, Microsoft offers its detailed replies to STAR, which are publicly available at the CSA website. Microsoft's reply incorporates ISO 27000 guidelines, and exemplifies the commitment Microsoft makes and importance Microsoft places on its customers' security and privacy.

Additional reading

- Cloud Security Alliance (CSA)
- COBIT Fact Sheet on the Information Systems Audit and Control Association (ISACA) website
- BSI Group – the British Standards Institution
- BS ISO/IEC 27005:2011 standard that provides guidelines for information security risk management
- International Organization for Standardization (ISO) Standards catalogue
- Global Foundation Services
- Windows Azure ISO Certification
- Microsoft Dynamics CRM ISO Certification
- White papers on Windows Azure
- Windows Azure Platform Legal Information
- Microsoft Dynamics CRM
- CSA STAR Registry
- Microsoft Office 365 Trust Center
- Windows Azure Trust CenterDirective 95/46/EC of the European Parliament and of the Council

TwC Next

Microsoft
One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security

www.microsoft.com/twcnext