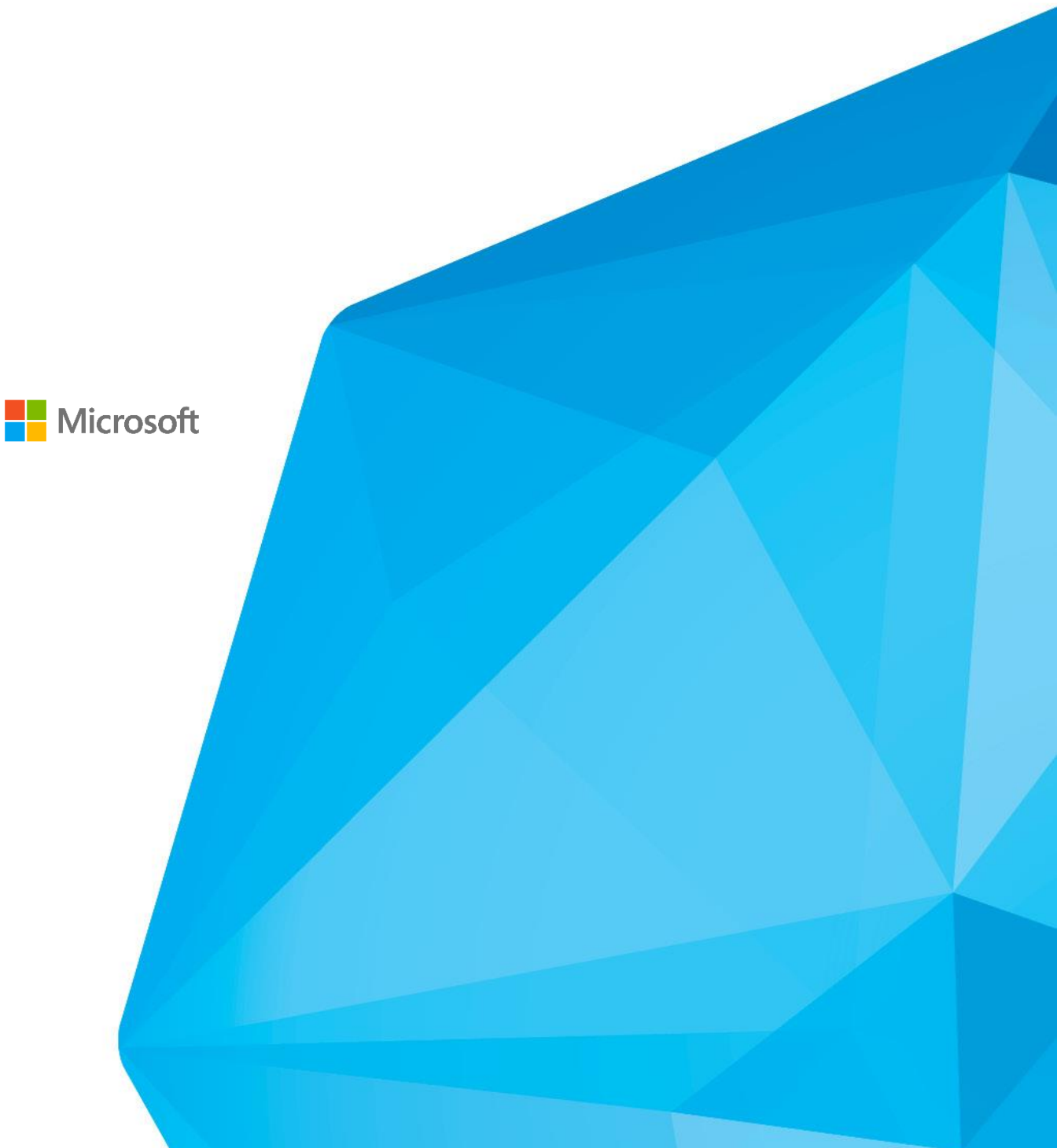
14 Cloud Security Controls for UK cloud

Using Microsoft Azure



Disclaimer

Published September 2016

Acknowledgements

Authors

Stuart Aston
Frank Simorjay

Contributors and reviewers

Glenn Pittaway
Tom Shinder
JB Im (CELA)
Jon Tobey (Wadeware)
Paul Henry (Wadeware)
Steve Wacker (Wadeware)

Table of Contents

Introduction

Microsoft Azure provides services that can help address the security and compliance needs of Microsoft customers. In addition, Microsoft works with customers to understand their assurance concerns, and to help define their responsibilities as well as its own with regard to protecting customer data and environmental infrastructure after services are provisioned. Such infrastructure includes applications, data content, virtual machines, access credentials, and compliance requirements.

In addition, in the wake of the recent landmark vote in the UK calling for the invocation of Article 50 of the Lisbon Treaty, customers should consider their implementation strategies for both on-premises and cloud-based services to ensure they meet their compliance obligations.

This paper provides insight into how Azure services align with the fourteen cloud security principles set forth in the CESG/NCSC [1]publication "Implementing the Cloud Security Principles," thereby enabling organisations to fast-track their ability to meet their compliance obligations using cloud-based services globally and in the UK.

Microsoft Azure is a growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and web—that allow customers to move faster, achieve more, and save money. Azure serves as a development, service hosting, and service management environment, providing customers with on-demand compute, storage, networking, and content delivery capabilities to host, scale, and manage applications on the Internet.

To get the most out of the Microsoft cloud platform, readers should be familiar with basic Azure and cloud computing concepts, as well as security and compliance fundamentals—they will not be discussed here. Links to additional materials can be found on the Get started with Azure webpage as well as through the Azure Trust Center and the Azure Security Information portal.

[1] In October 2016 the CESG has announced its merge with the National Cyber Security Center (NCSC), which will include the Information Security arm of GCHQ – the Centre for the Protection of National Infrastructure, CERT-UK and the Centre for Cyber Assessment.

Microsoft cloud principles of trust

Protecting the security, privacy, and integrity of sensitive customer data is one of Microsoft's highest priorities.

The Microsoft Trust Center (www.microsoft.com/TrustCenter) lists a number of underlying principles that guide the way Microsoft cloud services are built and operated, including:

- Security. Customers must be able to count on the security of their data. Security is built into Microsoft cloud services from the ground up, starting with the Security Development Lifecycle, a mandatory development process that embeds security requirements into every phase of the development process. Microsoft engineers help ensure that Microsoft cloud services are protected at the physical, network, host, application, and data layers so that all services are resilient to attack. Continuous proactive monitoring, penetration testing, and the application of rigorous security guidelines and operational processes further increase the level of detection and protection throughout Microsoft cloud services.
- Privacy. Customers must be able to trust that the privacy of their data will be protected and that it will be used only in ways that are consistent with their expectations. The Microsoft Online Services Privacy Statement describes the specific privacy policy and practices that pertain to customer data in Microsoft enterprise cloud services. Microsoft was also the first major cloud provider to adopt the first international code of practice for cloud privacy, ISO/IEC 27018.
- Transparency. Customers should know as much as possible about how their data is handled and to whom it is disclosed. Microsoft provides a wide range of evidence, including third-party audit reports and certifications for their respective services listed in the FAQ located on the Microsoft trust center. To verify that Microsoft meets the standards it sets for itself. The Microsoft Transparency Hub provides extensive information and statistics about how Microsoft has responded to law enforcement requests, US national security orders, and content removal requests.
- Compliance. Microsoft is committed to respecting and accommodating regional regulatory standards. To help organisations comply with national, regional, and industry-specific requirements that govern the collection and use of individuals' data, Microsoft offers the most comprehensive set of certifications and attestations of any cloud service provider.

Shared responsibilities

In Figure 1, the left-most column shows seven responsibilities (defined in the sections that follow) that organisations should consider, all of which contribute to the security and privacy of a computing environment.

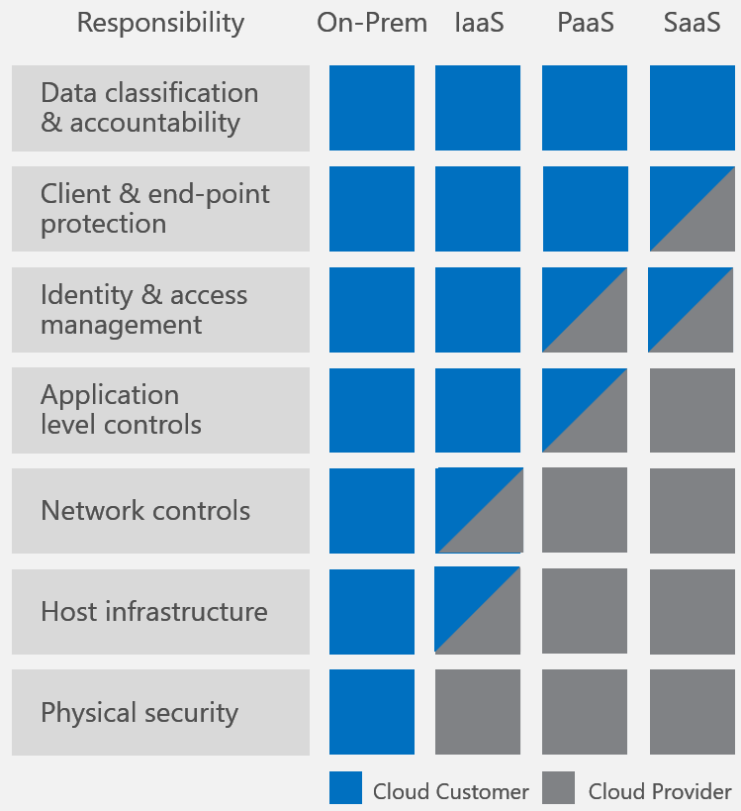


Figure 1. Shared responsibilities for security and privacy

After an information security management system (ISMS) foundation is set and best practices are adopted, there are additional areas to evaluate and understand to determine an organisation's risk posture and keys for mitigating its risks. To do this, organisations need to understand which areas are the cloud provider's responsibility and which are the organisation's responsibility. Figure 1 makes it clear that responsibilities are driven by the cloud service model (on-premises, IaaS, PaaS, SaaS).

With the exception of Data classification & accountability, customers and cloud service providers (CSPs) share responsibilities. Some responsibilities require CSPs and customers to manage and administer the responsibility together, including auditing of their domains. For example, consider Identity & access management when using Azure Active Directory Services. The configuration of services such as multi-factor authentication is up to the customer, but ensuring effective functionality is the responsibility of Microsoft Azure.

Government Cloud (G-Cloud) is a UK government initiative to ease procurement of cloud services by government departments and promote government-wide adoption of cloud computing. G-Cloud comprises a series of framework agreements with cloud services providers, such as Microsoft, and a listing of their services in an online store—the Digital Marketplace. This initiative enables public-sector organisations to compare and procure those services without having to carry out their own full review process. Inclusion in the Digital Marketplace requires a self-attestation of compliance, followed by a verification performed by the Government Digital Service (GDS) branch.

Instead of the central assessment of cloud services previously provided, the new process requires cloud service providers to self-certify and supply evidence in support of the 14 Cloud Security

Principles of G-Cloud (currently at version 6). This process has not changed either the evidence Microsoft produces or the standards that the company adheres to.

The Crown Commercial Service (an agency that works to improve commercial and procurement activity by the government) renewed the classification of Microsoft in-scope enterprise cloud services at G-Cloud v6, covering all of its offerings at the OFFICIAL level:

- Software as a service (SaaS). Using the cloud to deliver applications.
- Platform as a service (PaaS). Using the cloud to host, develop, and test applications.
- Infrastructure as a service (IaaS). Using the cloud in place of servers and other hardware.
- Cloud consulting services. Helping customers get the most from the cloud.

The inclusion of Microsoft services in the Digital Marketplace means that UK government agencies and partners can use in-scope services to store and process UK OFFICIAL government data, the majority of government data. In addition, there are now more than 450 Microsoft partners included in G-Cloud who are resellers of Microsoft cloud services. They can directly assert the compliance of in-scope services with the 14 cloud security principles in their own applications. Customers and partners, however, will need to achieve their own compliance for any components that are not included in the attestation and determination of compliance for Microsoft cloud services.

Addressing cloud security principles with Azure

In its publication "Cloud Security Guidance: Summary of Cloud Security Principles," CESG/NCSC , the information security arm of the Government Communications Headquarters (GCHQ) in the UK, laid out 14 security principles that organisations should use when evaluating cloud services, and which cloud service providers should consider when offering those services to government customers (referred to as "consumers" in the principles). The 14 principles are aligned with ISO 27001, an auditable, international, information security management standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001 formally defines requirements for a complete ISMS to help protect and secure an organisation's data. The principles defined by CESG/NCSC are:

1. Data in transit protection. Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.
2. Asset protection and resilience. Consumer data, and the assets that store or process it, should be protected against physical tampering, loss, damage, and seizure.
3. Separation between consumers. Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.
4. Governance framework. The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.
5. Operational security. The service provider should have processes and procedures in place to ensure the operational security of the service.
6. Personnel security. Service provider staff should be subject to personnel security screening and security education appropriate for their role.
7. Secure development. Services should be designed and developed to identify and mitigate threats to their security.
8. Supply chain security. The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.
9. Secure consumer management. Consumers should be provided with the tools required to help them securely manage their service.
10. Identity and authentication. Access to all service interfaces (for consumers and providers) should be limited to authenticated and authorised individuals.
11. External interface protection. All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.
12. Secure service administration. The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.

13. Audit information provision to consumers. Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.
14. Secure use of the service by the consumer. Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.

This paper describes how Azure addresses each of these cloud security principles, and provides information and advice that will help customers take full advantage of the security features offered by Azure. Microsoft is committed to providing organisations located inside and outside of the UK that their data will be kept secure and their privacy protected at the same levels that existed prior to the invocation of Article 50 of the Lisbon Treaty.

The UK Governments 14 Cloud Security principles

1. Data in transit protection

Consumer data transiting networks should be adequately protected against tampering and eavesdropping (confidentiality). If this principle is not implemented, the integrity or confidentiality of the data may be compromised whilst in transit.

Azure uses the industry-standard Transport Layer Security (TLS) 1.2 protocol with 2048-bit RSA/SHA256 encryption keys, as recommended by CESG/NCSC , to encrypt communications both between the customer and the cloud, and also internally between Azure systems and data centers. For example, when administrators use the Microsoft Azure Portal to manage the service for their organisation, the data transmitted between the portal and the administrator's device is sent over an encrypted TLS channel. When an email user connects to Outlook.com using a standard web browser, the HTTPS connection provides a secure channel for receiving and sending email.

Azure offers its customers a range of options for securing their own data and traffic. The certificate management features built into Azure give administrators flexibility for configuring certificates and encryption keys for management systems, individual services, secure shell (SSH) sessions, virtual private network (VPN) connections, remote desktop (RDP) connections, and other functions.

Developers can use the cryptographic service providers (CSPs) built into the Microsoft .NET Framework to access Advanced Encryption Standard (AES) algorithms, along with Secure Hash Algorithm (SHA-2) functionality to handle such tasks as validating digital signatures. Azure Key Vault helps customers safeguard cryptographic keys and secrets by storing them in hardware security modules (HSMs).

Resources:

- Client-Side Encryption and Azure Key Vault for Microsoft Azure Storage.
- Data access and protection considerations for all devices, including BYOD (bring your own device).
- Service Management REST API Reference for Azure.
- .NET Framework Cryptography Model. Azure is built on the .NET framework and provides customers with access to the same strong cryptographic protocols and straightforward key management methods incorporated into the .NET security model.
- Validated VPN devices for implementing site-to-site VPN connections to Azure. Also see ExpressRoute, a streamlined solution for establishing a secure private connection between customer infrastructure and Azure datacenters.
- Configuring SSL for an application in Azure.

2. Asset protection and resilience

Consumer data, and the assets that store or process such data, should be protected against physical tampering, loss, damage, and seizure. If this principle is not implemented, inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction,

or reputational damage.

CESG/NCSC defines the following aspects to consider when implementing or assessing this principle:

- Physical location and legal jurisdiction. *The locations at which consumer data is stored, processed and managed from, must be identified so that organisations can understand the legal circumstances in which their data could be accessed without their consent.*
- Data center security. *The locations used to provide cloud services need physical protection against unauthorized access, tampering, theft and reconfiguration of systems. Inadequate protections may result in the disclosure, alteration, or loss of data.*
- Data at rest protection. *Consumer data should be protected when stored on any type of media or storage within a service to ensure that it is not accessible by local unauthorized parties. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost, or stolen media.*
- Data sanitization. *The process of provisioning, migrating, and de-provisioning resources should not result in unauthorized access to consumer data.*
- Equipment disposal. *Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way that does not compromise the security of the service or consumer data stored in the service.*
- Physical resilience and availability. *Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents, or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, with attendant business impacts.*

Physical location and legal jurisdiction

Most Azure services are deployed regionally, and customers can configure certain Azure services to store customer data only in a single region. In late 2016, Microsoft launched two new regions, United Kingdom South and United Kingdom West, for the convenience of customers who wish to have their data stored in the UK. See Microsoft Azure — Where is my customer data? for details about how Microsoft treats customer data stored regionally.

Azure infrastructure includes hardware, software, networks, administrative and operations staff, and the physical datacenters that house it all.

Datacenter security

Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft online services. Each facility is designed to run 24x7x365 and employs various industry-standard measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

Data at rest protection

Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily and cost effectively

maintain control of keys used by cloud applications and services to encrypt data. Azure Disk Encryption enables customers to encrypt virtual machines. Azure Storage Service Encryption makes it possible to encrypt all data placed into a customer's storage account.

Data sanitization

When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before reuse. As part of agreements for cloud services such as Azure Storage, Azure VMs, and Azure Active Directory, Microsoft contractually commits to timely deletion of data.

Equipment disposal

Upon a system's end-of-life, Microsoft operational personnel follow rigorous data handling procedures and hardware disposal processes to help assure that no hardware that may contain customer data is made available to untrusted parties.

Physical resilience and availability

Regional pairs are enabled by default in Windows Azure Storage, helping to ensue that applications are resilient during datacenter failures. In regional pairing, Azure asynchronously replicates data from a primary location to a secondary location within the same region. An Azure region is an area within a geography containing one or more datacenters. This concept is shown in the following figure.

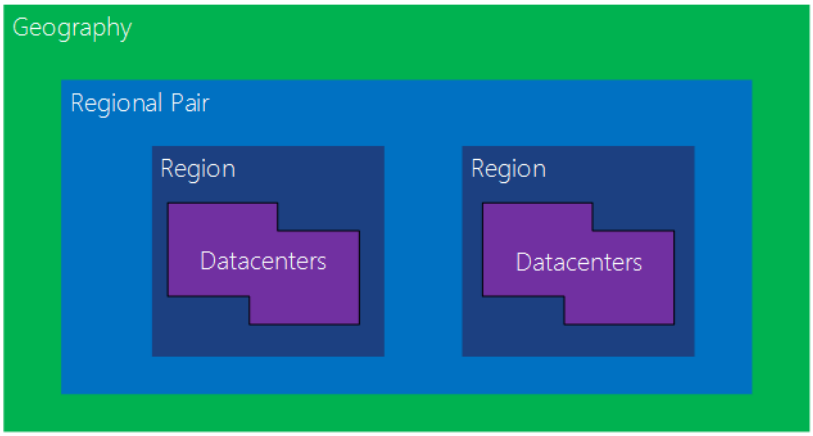


Figure 2. Azure regional pairs

Another type of resiliency is applications resiliency, which helps ensure that during either a planned or unplanned maintenance event, at least one virtual machine will be available and meet the 99.95% Azure SLA. See "Manage the availability of virtual machines" for more information.

Resource:

- The CSA published the Cloud Control Matrix to support customers in the evaluation of cloud providers and to identify questions that should be answered before moving to cloud services. In response, Microsoft Azure answered the CSA Consensus Assessment Initiative Questionnaire CSA CAIQ to describe how Microsoft addresses the suggested principles.

3. Separation between consumers

Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another. If this principle is not implemented, service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.

Because all customer cloud servers are virtual, the physical separation paradigm no longer applies. Microsoft Azure was designed to help identify and counter risks inherent in a multitenant environment. Data storage and processing is logically segregated among consumers of Azure using Active Directory and functionality specifically developed for multitenant services, which aims to ensure that consumer data stored in shared Azure data centers is not accessible by another organisation.

Fundamental to any shared cloud architecture is the isolation provided for each consumer to prevent one malicious or compromised consumer from affecting the service or data of another. In Azure, one customer's subscription can include multiple deployments, and each deployment can contain multiple VMs. Azure provides network isolation at several points:

- Deployment. Each deployment is isolated from other deployments. Multiple VMs within a deployment are allowed to communicate with each other through private IP addresses.
- Virtual network. Multiple deployments (inside the same subscription) can be assigned to the same virtual network, and then allowed to communicate with each other through private IP addresses. Each virtual network is isolated from other virtual networks.
- Traffic between VMs always traverses through trusted packet filters.
- Protocols such as Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), and other OSI Layer-2 traffic from a VM are controlled using rate-limiting and anti-spoofing protection.
- VMs cannot capture any traffic on the network that is not destined for them.
- Customer VMs cannot send traffic to Azure private interfaces, or other customers' VMs, or Azure infrastructure services themselves. Customer VMs can only communicate with other VMs owned or controlled by the same customer and with Azure infrastructure service endpoints meant for public communications.

To verify isolation on the platform:

- Microsoft conducts ongoing penetration tests of the environment in accordance with the dynamic nature of the cloud to help ensure that a consumer's data remains private to them.
- Residual risks are published in the Microsoft Risk Management and Accreditation Document Set (RMADS) and Residual Risk statement, which are available under nondisclosure agreement (NDA) from Microsoft.

4. Governance framework

The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it. If this principle is not implemented, any procedural, personnel, physical, and technical controls in place will not

remain effective when responding to changes in the service and to threat and technology developments. Cloud service providers should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.

The Microsoft compliance framework includes a standard methodology for defining compliance domains, determining which objectives apply to a given team or asset, and capturing how domain control objectives are addressed in sufficient detail as they apply to a given set of industry standards, regulations, or business requirements. The framework maps controls to multiple regulatory standards, which enables Microsoft to design and build services using a common set of controls, thereby streamlining compliance across a range of regulations today and as they evolve in the future.

Microsoft compliance processes also make it easier for customers to achieve compliance across multiple services and meet their changing needs efficiently. Together, security-enhancing technology and effective compliance processes enable Microsoft to maintain and expand a rich set of third-party certifications. These certifications help customers demonstrate compliance readiness to their customers, auditors, and regulators.

The Microsoft compliance framework includes the following activities:

- Identify and integrate requirements. Scope and applicable controls are defined. Standard operating procedures (SOP) and process documents are gathered and reviewed. In the standard plan–do–check–act management methodology that is well known in process development, this activity aligns with the "Plan" phase.
- Assess and remediate gaps. Gaps in process or technology controls are identified and remediated, including the implementation of new administrative and technical controls. Aligns with the "Do" phase.
- Test effectiveness and assess risk. Effectiveness of controls is measured and reported. On a consistent and regular basis, independent internal audit groups and external assessors review internal controls. Compliance with internal security standards and requirements, such as verification that product groups adhere to the Microsoft Security Development Lifecycle (SDL), occurs in this phase. Aligns with the "Check" phase.
- Attain certification and attestations. Engagement with third-party certification authorities and auditors occurs. Aligns with the "Act" phase.
- Improve and optimize. If issues or non-conformities are found, the reason is documented and assessed further. Such findings are tracked until fully remediated. This phase also involves continuing to optimize controls across security domains to generate efficiencies in passing future audit and certification reviews. Aligns with the "Act" phase.

Azure complies with a broad set of international as well as regional and industry-specific compliance standards, such as ISO 27001, FedRAMP, SOC 1, and SOC 2. Compliance with the strict security controls contained in these standards is verified by rigorous third-party audits that demonstrate Azure services work with and meet world-class industry standards, certifications, attestations, and authorizations.

Azure is designed with a compliance strategy that helps customers address business objectives as well

as industry standards and regulations. The security compliance framework includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis to achieve certificates and attestations.

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

- 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.
- CSA CCM. The Cloud Security Alliance (CSA) is a non-profit, member-driven organisation 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 fulfills the security, privacy, compliance, and risk management requirements defined in the CCM version 3.0.1., 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 European Union. 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 approval ensures that Azure customers can use Microsoft services to move data freely through the Microsoft cloud from Europe to the rest of the world.
- ISO/IEC 27018. Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, which deals with 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.
- PCI DSS. Azure is Level 1 compliant with Payment Card Industry (PCI) Data Security Standards (DSS) version 3.0, the global certification standard for organisations 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.

Resource:

- 13 Effective Security Controls for ISO 27001 Compliance when using Microsoft Azure. This paper provides insight into how organisations can use thirteen security principles helps address critical security and compliance controls, and how these controls can fast track an organisation's ability to meet its compliance obligations using cloud-based services.

5. Operational security

The service provider should have processes and procedures in place to ensure the operational security of the service. If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect, or prevent attacks against it.

CESG/NCSC defines the following aspects to consider when implementing or assessing this principle:

- Configuration and change management. *Good configuration management processes should ensure that knowledge of the assets which make up the service, along with their configuration and dependencies, are known and accurate. Good change management processes should ensure any changes to the service (which could have an effect on its security) are identified and managed. They should also lead to detection of unauthorized changes.*
- Vulnerability management. *Occasionally, vulnerabilities will be discovered which, if left unmitigated, will pose an unacceptable risk to the service. Robust vulnerability management processes are required to identify, triage, and mitigate vulnerabilities.*
- Protective monitoring. *Effective protective monitoring allows a service provider to detect and respond to attempted and successful attacks, misuse, and malfunction. A service which does not effectively monitor for attacks and misuse will be unlikely to detect attacks (both successful and unsuccessful) and will be unable to quickly respond to potential compromises of consumer environments and data.*

Operational Security Assurance (OSA) is a framework that incorporates the knowledge gained through a variety of resources that are unique to Microsoft, such as the Microsoft Security Response Center (MSRC), and incorporates deep awareness of the cybersecurity threat landscape. OSA combines this knowledge with the experience of running hundreds of thousands of servers in data centers around the world that deliver more than 200 online services to more than 1 billion customers and 20 million businesses in 88 countries.

Microsoft uses OSA to minimize risk by helping to ensure that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are actually being followed effectively. When issues arise, a feedback loop helps ensure that future revisions of OSA contain mitigations to address them.

OSA helps make Microsoft cloud-based services' infrastructure more resilient to attack by decreasing the amount of time needed to prevent, detect, contain, and respond to real and potential Internet-based security threats, thereby increasing the security of those services for customers.

Vulnerability management

Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure is also able to draw on the resources of the Microsoft Security Response Center (MSRC), which identifies, monitors, responds to, and resolves security incidents and cloud vulnerabilities around the clock, each day of the year.

Protective monitoring

Microsoft 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 with internal and external partners alike. See Principle 11 for more details about how Microsoft responds to attempted attacks on Azure systems.

Resources:

- Operational Security for Online Services Overview. This white paper provides insight into how Microsoft applies its resources to online services in ways that extend beyond traditional standards and methodology to deliver industry-leading capabilities.
- Data classification for cloud readiness. This paper presents guidance for categorizing stored data by sensitivity and business impact in order to determine the risks associated with the data.
- Standard Response to Request for Information: Microsoft Azure Security, Privacy, and Compliance. Details how Azure complies with the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) operational security requirements.

6. Personnel security

Service provider staff should be subject to personnel security screening and security education for their role. If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased.

Microsoft Azure Operations and Customer Support personnel and data center staff, who operate Azure services and provide customer support (or Microsoft subcontractors who assist with platform operations, troubleshooting, and technical support) undergo a Microsoft standard background (or equivalent) check to evaluate employee education, employment, and criminal history. The background checks that are carried out are broadly in line with the requirements of the UK Government's BPSS / BS7858. They do not specifically include a formal identity check.

Microsoft includes nondisclosure provisions in its employee and subcontractor contracts. All appropriate Microsoft employees and subcontractors take part in a Microsoft Azure sponsored security-training program that informs staff of their responsibilities for information security.

Microsoft Azure services staff suspected of committing breaches of security and/or violating the Information Security Policy (equivalent to a Microsoft Code of Conduct violation) are subject to an investigation process and appropriate disciplinary action up to and including termination. Contracting staff suspected of committing breaches of security and/or violations of the Information Security Policy are subject to formal investigation and action appropriate to the associated contract, which may include termination of such contracts. If the circumstances warrant it, Microsoft may refer the matter for prosecution by a law enforcement agency.

To supplement this system of background checks and security education, Microsoft deploys combinations of preventive, defensive, and reactive controls to help protect against unauthorized developer and/or administrative activity, including the following mechanisms:

- Tight access controls on sensitive data, including a requirement for two-factor smartcard-based authentication to perform sensitive operations.

- Combinations of controls that enhance independent detection of malicious activity.
- Multiple levels of monitoring, logging, and reporting.

7. Secure development

Services should be designed and developed to identify and mitigate threats to their security. If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service, or enable other malicious activity.

Cloud service providers need to use good development practices to ensure the secure delivery of services to its customers. The Microsoft Security Development Lifecycle (SDL) provides an effective threat-modeling process to identify threats and vulnerabilities in software and services. Threat modeling is a team exercise, encompassing the operations manager, program/project managers, developers, and testers, and represents a key security analysis task performed for solution design. This approach should also be considered by customers developing their own applications to be hosted in cloud services, either using IaaS or PaaS. Team members use the SDL Threat Modeling Tool to model all services and projects, both when they are built and when they are updated with new features and functionality. Threat models cover all code exposed on the attack surface and all code written by or licensed from a third party, and consider all trust boundaries. The STRIDE system (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) is used to help identify and resolve security threats early in the design process, before they can affect customers.

8. Supply chain security

The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement. If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.

Cloud services often rely upon third-party products and services. Those third parties can have an impact on the overall security of the services. If the supply chain principle is not implemented, it is possible that supply chain compromise could undermine the security of the service and affect the implementation of other security principles.

In Azure, security risks that relate to external parties, such as customers and vendors, are identified and addressed as follows:

- Third parties undergo a review process and an approved vendor list is established and used. These vendors are required to comply with Microsoft security policies and are audited.
- Additional risks that relate to granting access to facilities and information systems are controlled and managed by Microsoft teams, including physical and network level access to facilities and Microsoft resources.

Customers must also be ready to evaluate all elements in their supply chain. To this end, Microsoft provides evidence of compliance through third-party auditors. A customer with an Azure Active Directory account or a trial subscription to Microsoft Azure, Office 365, or Dynamics CRM Online

can access the Service Trust Portal directly. They will be asked to provide their credentials. Access credentials are managed through the organisation's cloud global administrator. Visit the Service Trust Portal for specific details on accessing the portal. The Service Trust Portal offers access to a deep set of security, privacy, and compliance resources, such as independent audit reports of Microsoft cloud services, risk assessments, security best practices, and other similar materials, including:

- SOC 1 and SOC 2 auditor's reports
- ISO 27001 and ISO 27018 audit reports and scope statements
- Office 365 Information Security Management System (ISMS) guidance

Resources:

- Review Monitoring partner solutions with Azure Security Center. This document describes how Azure Security Center provides the ability to monitor at a glance the health status of partner solutions that are integrated with an Azure subscription.
- Microsoft Supplier Program. Details the requirements Microsoft suppliers must meet, including the Supplier Security & Privacy Assurance Program and the Supplier Code of Conduct.
- Microsoft Supplier Data Protection Requirements. Applies to all Microsoft suppliers that collect, use, distribute, access, or store Microsoft Personal Information or Microsoft Sensitive Information.
- Customers can visit the Service Trust Portal to download compliance reports.

9. Secure consumer management

Consumers should be provided with the tools required to help them securely manage their service. If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications, and data.

CESG/NCSC defines the following aspects to consider when implementing or assessing this principle:

- Authentication of consumers to management interfaces and within support channels. *In order to maintain a secure service, consumers need to be securely authenticated before being allowed to perform management activities, report faults, or request changes to the service.*
- Separation and access control within management interfaces. *Many cloud services are managed via web applications or APIs. These interfaces are a key part of the service's security. If consumers are not adequately separated within management interfaces, one consumer may be able to affect the service or modify data belonging to another.*

Authentication of consumers to management interfaces and within support channels

Customers administer their Azure resources through the Azure portal, which provides access to all virtual machines, databases, cloud services, and other resources configured for the customer's account. Web access to the Azure portal is secured by industry-standard Transport Layer Security (TLS) 1.2 connections using 2048-bit RSA/SHA256 encryption keys, as recommended by CESG/NCSC . Role-based access controls are provided to enable customers to provide limited access to Azure management resources for specific users and groups.

Separation and access control within management interfaces

As outlined in separation between consumers separation is built into Azure at its core. Azure Active Directory (Azure AD) can be used to provide every user who authenticates to the Azure portal with access to only the resources they are entitled to see and manage. As a result, different customer accounts are strictly segregated from one another when managed through the common Azure portal.

Resources:

- Microsoft Azure portal. Explore the features of the Azure portal, including a walkthrough of its components.
- Role-based access control in the Azure portal. Learn about using role-based assignments to manage access to an Azure subscription.

10. Identity and authentication

Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals. If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data, or denial of service may occur.

Azure provides services to help track identity as well as integrate it with identity stores that may already be in use. Azure AD is a comprehensive identity and access management service for the cloud that helps secure access to data in on-premises and cloud applications. Azure AD also simplifies the management of users and groups by combining core directory services, advanced identity governance, security, and application access management.

Resources:

- The fundamentals of Azure identity management. Details about how identity is used and managed in Azure.
- Use role-based access control to manage access to your Azure subscription resources
- Azure AD Privileged Identity Management. Provides a mechanism for managing and monitoring administrators in Azure AD and granting temporary, "just-in-time" administrative access to users for ad hoc tasks for short predetermined periods.
- Multi-factor authentication. Adds an additional layer of security for Azure data and applications. Functionality for both cloud and on-premises applications.
- Azure AD Conditional Access. Allows the configuration of per-application multi-factor authentication access rules for SaaS applications and Azure AD connected apps.

11. External interface protection

All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them. If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it.

Microsoft employs a method it calls "Red Teaming" to improve Azure security controls and processes

through regular penetration testing. The Red Team is a group of full-time staff within Microsoft that focuses on performing targeted and persistent attacks against Microsoft infrastructure, platforms, and applications, but not end-customers' applications or data.

The job of the Red Team is to simulate the kinds of sophisticated, well-funded targeted attack groups that can pose a significant risk to cloud services and computing infrastructures. To accomplish this simulation, the team researches and models known persistent adversaries, in addition to developing their own custom penetration tools and attack methods.

Because of the sensitive and critical nature of the work, Red Team members at Microsoft are held to very high standards of security and compliance. They go through extra validation, background screening, and training before they are allowed to engage in any attack scenarios. Although no end-customer data is deliberately targeted by the Red Team, they maintain the same Access To Customer Data (ATCD) requirements as service operations personnel that deploy, maintain, and administer Microsoft Azure and Office 365. The Red Team abides by a strict code of conduct that prohibits intentional access or destruction of customer data, or disruptions to customer Service Level Agreements (SLAs).

A different group, the Blue Team, is tasked with defending Azure services and infrastructure from attack, not only from the Red Team but from any other source as well. The Blue Team is comprised of dedicated security responders as well as representatives from Engineering and Operations. The Blue Team follows established security processes and uses the latest tools and technologies to detect and respond to attacks and penetration. The Blue Team does not know when or how the Red Team's attacks will occur or what methods may be used—in fact, when a breach attempt is detected, the team does not know if it is a Red Team attack or an actual attack from a real-world adversary. For this reason, the Blue Team is on-call 24x7, 365 days a year, and must react to Red Team breaches the same way it would for any other adversary.

Microsoft understands that security assessment is also an important part of customer application development and deployment. Therefore, Microsoft has established a policy for customers to carry out authorized penetration testing on their applications hosted in Azure. Because such testing can be indistinguishable from a real attack, it is critical that customers conduct penetration testing only after notifying Microsoft. Penetration testing must be conducted in accordance with Microsoft terms and conditions.

Resources:

- Microsoft Enterprise Cloud Red Teaming. Explores the Red Teaming method, how attacks are conducted and defended against, and the history and rationale behind the practice.
- Red vs. Blue - Internal security penetration testing of Microsoft Azure. A brief video explaining the Azure penetration testing approach and discussing the roles of the Red and Blue teams.
- Azure customer penetration testing overview. Explains the process by which customers may conduct penetration tests on their own Azure infrastructures, and provides a form for customers to notify and request permission from Microsoft for such tests.

12. Secure service administration

The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service. If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.

The current threat environment for organisations is rife with sophisticated phishing and other Internet attacks that create continuous risk of security compromise for Internet-exposed accounts and workstations. This threat environment requires an organisation to adopt an "assume breach" security posture when designing protections for high-value assets such as administrative accounts and sensitive business assets. These high-value assets need to be protected against both direct Internet threats as well as attacks mounted from other workstations, servers, and devices in the environment.

To help protect against such attacks, Azure infrastructure operations personnel are required to use secure admin workstations (SAWs; also known as privileged access workstations, or PAWs). The SAW approach is an extension of the well-established recommended practice to use separate admin and user accounts for administrative personnel. This practice uses an individually assigned administrative account that is completely separate from the user's standard user account. SAW builds on that account separation practice by providing a trustworthy workstation for those sensitive accounts.

Resources:

- Security Management in Azure. Provides guidance for Azure customers on administering their accounts securely
- Protecting high-value assets with secure admin workstations. Includes details about how SAWs are used at Microsoft
- Privileged Access Workstations. Information and instructions for constructing secure workstations to manage high-value assets

13. Audit information provision to consumers

Consumers should be provided with the audit records they need to monitor access to their service and the data held within it. If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.

Azure Log Analytics collects records of the events occurring within an organisation's systems and networks as soon as they occur, before anyone can tamper with them, and allows different types of analysis by correlating data across multiple computers. Azure enables customers to perform security event generation and collection from Azure IaaS and PaaS roles to central storage in their subscriptions. These collected events can be exported to on-premises security information and event management (SIEM) systems for ongoing monitoring. After the data is transferred to storage, there are many options to view the diagnostic data.

Azure built-in diagnostics can help with debugging. For applications that are deployed in Azure, a set of operating system security events are enabled by default. Customers can add, remove, or modify events to be audited by customizing the operating system audit policy.

At a high level, it is quite easy and simple to begin collecting logs using Windows Event Forwarding (WEF) or the more advanced Azure Diagnostics when Windows-based VMs are deployed using IaaS in Azure. In addition, Azure Diagnostics can be configured to collect logs and events from PaaS role instances. When using IaaS-based VMs, a customer simply configures and enables the desired security events the same way they enable Windows Servers to log audits in their on-premises datacentre. For web applications, it's also possible to enable IIS logging if that is the primary application and deployment in Azure. Customers can always store security data in storage accounts in supported geo-locations of their choice to meet data sovereignty requirements.

Resources:

- Azure security and audit log management. Describes how to set up logging effectively to monitor an Azure subscription.
- Azure Status. Monitor the health of Azure services worldwide.
- How to Monitor a Media Services Account. Explains how the Azure Media Services Dashboard can be used to obtain metrics and account information for a Media Services account.
- How to Monitor Cloud Services
- Monitor a storage account in the Azure Portal
- Monitor Apps in Azure App Service
- Monitor Hadoop clusters in HDInsight using the Ambari API.
- Monitor Azure data factories using Data Factory .NET SDK.

14. Secure use of the service by the consumer

Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected. If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers.

Server misconfiguration is one of the most common causes for unauthorized users accessing and compromising the host. Because of the potentially complex security configuration requirements, it's essential to use a master server image that has security measures in place. Azure provides customers a marketplace with a gallery of servers that have been configured with security in mind. However, the use of the servers in the marketplace requires attention both for when organisations require custom security modifications and also to prevent security configuration drift.

Azure Security Center helps consumers prevent, detect, and respond to threats with increased visibility into and control over the security of their Azure resources. It provides integrated security monitoring and policy management across Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.

- Prevention. Security Center can be used to monitor the security state of Azure resources, define policies for subscriptions and resource groups, implement policy-driven security recommendations, and rapidly deploy security services and appliances from Microsoft and partners.

- Detection. Security Center can automatically collect and analyses security data from Azure resources, the network, and partner solutions such as antimalware programs and firewalls. It takes advantage of global threat intelligence from Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds, and applies advanced analytics, including machine learning and behavioral analysis.
- Respond. Security Center provides prioritized security incidents/alerts, offers insights into the source of the attack and affected resources, and suggests ways to stop the current attack and help prevent future attacks

Conclusion

Cloud computing offers tremendous opportunities to enable increased quality and greater access at lower cost of services. These advantages must be balanced against the complexity of managing security and privacy in multi-tenanted cloud services and how an organisation shows the appropriate compliance to applicable standards. Internal frameworks such as OSA and SDL, deep experience with cloud computing, and compliance with such international standards as ISO 27001 provide Microsoft with the ability to help organisations evaluate their overall privacy, security, and regulatory compliance posture for the specific UK government requirements "Implementing the Cloud Security Principles." The information in this document is provided as a way to approach that migration, including: compliance requirements, shared responsibilities, and rationalized mapping to address necessary controls.