timeware® in the cloud:
Security

timeware®

NMD³ Hosting

timeware®

NMD³ Hosting

Contents

timeware®

NMD³ Hosting

Introduction

This document highlights the cloud security guidance outlined by the UK National Cyber Security Centre for larger businesses and enterprises, including the public sector.

The National Cyber Security Centre cloud security guidance website can be found here:

https://www.ncsc.gov.uk/collection/cloud

In relation to the development and implementation of 'timeware® in the cloud', we have responded to each of the National Cyber Security Centre 14 principles, by commenting on the solutions and services provided by Azure and the product designs implemented by Lead Developer and Technical Directort, Nathan Price.

For further information about the solutions, please email admin@nmd3hosting.com.

Principle 1: Data in transit protection

User data transiting networks should be adequately protected against tampering and eavesdropping.

Data in transit protection should be achieved through a combination of:

encryption – denying your attacker the ability to read or modify data

network protection – denying your attacker the ability to intercept data

authentication – denying your attacker the ability to impersonate the service

Goals

You should be sufficiently confident that:

- data is protected in transit between your end user device(s) and the service
- data is protected in transit as it flows between internal components within the service
- data is protected in transit where exposed to other external services, such as via an API

You should prefer a cloud provider that:

- encrypts all customer-data in transit by default
- pre-configures data in transit encryption, and defaults to the latest industry standards
- uses standardised, well-understood algorithms and protocols (such as TLS and IPsec) to protect data
- makes it easy to implement good data in transit protections in your application

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-1-data-in-transit-protection

Principle 1: Data in transit protection - Our Comment

Data in transit protection is a crucial aspect of cybersecurity, especially when using cloud services like Microsoft Azure. When we talk about "data in transit," we're referring to data that is being transferred over a network – as opposed to "data at rest," which is data that is stored on a disk or in a database.

In the context of Azure, data in transit protection involves several key components:

1. **Encryption:** This is the primary method of protecting data in transit. Azure uses industry-standard protocols such as TLS (Transport Layer Security) and SSL (Secure Sockets Layer) to encrypt data as it travels between Azure data centres and the users. This encryption ensures that even if the data is intercepted, it cannot be read by unauthorised parties.
2. **Secure Transfer Protocols:** Azure supports secure transfer protocols like HTTPS, FTPS, and SFTP for data transmission. These protocols provide additional security measures such as authentication, data integrity checks, and encryption.
3. **VPN and ExpressRoute:** For secure, private connections to Azure, you can use Virtual Private Networks (VPNs) or Azure ExpressRoute. VPNs encrypt data traffic over public networks, while ExpressRoute provides a direct, private connection to Azure, bypassing the public internet entirely.
4. **Application-level Security:** Beyond the network level, Azure provides tools and guidelines for securing data at the application level. This includes best practices for secure coding, using Azure Application Gateway for SSL termination, and leveraging Azure services like Azure Active Directory for authentication and authorisation.
5. **Monitoring and Threat Detection:** Azure provides extensive monitoring and threat detection capabilities. Services like Azure Security Centre and Azure Monitor help in detecting and responding to security threats in real time, including potential threats to data in transit.
6. **Compliance and Standards:** Azure complies with various international and industry-specific standards such as ISO 27001, HIPAA, and PCI DSS. This compliance ensures that data in transit is protected according to globally recognised standards.
7. **End-to-End Encryption Options:** For scenarios requiring heightened security, Azure offers end-to-end encryption options where encryption occurs at the client-side, and the data remains encrypted throughout its journey until it reaches the intended recipient.

By implementing these measures, Azure ensures that data in transit is protected against eavesdropping, tampering, and other forms of cyberattacks, which is vital for maintaining the confidentiality and integrity of sensitive information.

Principle 2: Asset protection and resilience

Your data (and the assets storing or processing it) should be adequately protected.

Data types that are often overlooked include credentials, configuration data, derived metadata and logs. These must also be appropriately protected.

You should consider:

1. Physical location and legal jurisdiction
2. Data centre security
3. Data encryption
4. Data sanitisation and equipment disposal
5. Physical resilience and availability

Principle 2.1: physical location and legal jurisdiction

Goals

You should be confident that you know where your data is, and who can access your data. This should include derivatives of your data, such as verbose logs and machine learning models, unless sensitive aspects have been intentionally excluded or removed.

You should understand:

- in which countries your data will be stored, processed and managed
- which legal jurisdiction(s) your data will be subject to, and whether this is acceptable to you
- the rights that the service provider will have to access and use your data
- the legal circumstances under which your data could be accessed without your consent, and how this affects your compliance with UK legislation

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-2-asset-protection-and-resilience

Principle 2: Asset protection and resilience - Our comment

When using Microsoft Azure, understanding the physical location of data and the legal jurisdiction under which it falls is essential for several reasons, including data sovereignty, compliance with local and international laws, and performance considerations. Here's an overview:

1. **Physical Location of Data Centres:** Microsoft Azure operates a global network of data centres across various regions and countries. These data centres host the physical servers and infrastructure where customer data is stored and processed. The location of these data centres can impact data latency, redundancy, and availability.
2. **Choosing a Region:** When you create a resource in Azure, you select a region where that resource will be located. This decision can be based on factors like proximity to users (to reduce latency), compliance with specific data residency and sovereignty laws, or the availability of certain Azure services and features in different regions.
3. **Data Residency and Sovereignty:** Data residency refers to the physical location of data in a specific country or region. Data sovereignty extends this concept to the legal aspects, implying that data is subject to the laws and governance structures of the country in which it is physically located. This is particularly important for organisations that must comply with specific legal requirements regarding where their data is stored and processed.
4. **Legal Jurisdiction:** The legal jurisdiction of data refers to the legal system and laws that govern the data stored in a particular location. This includes laws related to data protection, privacy (like the GDPR in Europe), and government access to data. The jurisdiction can affect how data is managed, who can access it, and under what circumstances.
5. **Compliance and Certifications:** Microsoft Azure offers a range of compliance options to meet various regional and industry-specific requirements. Azure's compliance offerings are comprehensive and include certifications and attestations such as ISO 27001, HIPAA, FedRAMP, GDPR, and many others. Customers can choose to deploy services in specific regions to meet these compliance requirements.
6. **Data Transfer and Replication:** Azure allows data to be replicated for redundancy and high availability. However, this replication is generally within the same region or between specified regions. Customers concerned about data sovereignty need to be aware of and manage how their data is replicated and where it is stored.
7. **Contractual and Policy Considerations:** When using Azure, customers are bound by the terms of the Microsoft Online Services Terms (OST) and Data Protection Addendum (DPA), which outline the responsibilities and commitments regarding data handling, protection, and legal compliance.
8. **Transparency and Control:** Microsoft provides transparency about where data is stored and offers tools and policies that give customers control over their data's location. For example, the Azure Policy service can be used to enforce rules about where resources are deployed.

Understanding the physical location and legal jurisdiction of data in Azure is crucial for organisations to ensure they meet legal obligations, protect data privacy, and optimise system performance. This understanding aids in making informed decisions about resource deployment, data management, and compliance strategy in the cloud.

Principle 2.2: data centre security

Goals

You should be confident that the physical security measures employed by the provider are sufficient to protect against unauthorised access, tampering, theft or reconfiguration of systems, when considered alongside data at rest protections.

Principle 2.2: data centre security - Our comment

Data centre security in Microsoft Azure is a critical aspect of its overall cloud security strategy. Azure employs a comprehensive, multi-layered approach to secure its data centres and the infrastructure within them. This approach includes a blend of physical, logical, and procedural safeguards. Here's an overview:

1. **Physical Security:**
   - **Access Control:** Azure data centres are equipped with robust access control systems. Access to these facilities is strictly controlled and limited to authorised personnel only. This includes the use of biometric scanners, smart cards, and pin codes.
   - **Surveillance:** Continuous video surveillance and security alarms are standard across Azure data centres. This surveillance is monitored 24/7 by security personnel.
   - **Physical Barriers:** Data centres are protected by multiple physical barriers, including fencing, security gates, and bullet-resistant walls.
   - **Security Personnel:** Trained security guards are present on-site 24/7 to monitor and respond to any security incidents.
   - **Environmental Controls:** Data centres are equipped with environmental controls to safeguard the hardware from fire, flooding, and other environmental hazards. This includes advanced fire detection and suppression systems.
2. **Logical and Network Security:**
   - **Network Segmentation and Firewalls:** Internal data centre networks are segmented and protected by robust firewalls. This segmentation limits potential lateral movement in the event of a breach.
   - **Intrusion Detection and Prevention Systems (IDPS):** These systems are used to monitor and analyze network traffic for signs of malicious activity or policy violations.
   - **DDoS Protection:** Azure provides built-in defenses against Distributed Denial of Service (DDoS) attacks to maintain service availability.
3. **Operational Security:**
   - **Background Checks:** Personnel with access to data centre facilities undergo thorough background checks as part of the hiring process.
   - **Security Training:** Regular security training is mandatory for all staff, ensuring they are aware of and can effectively implement security protocols.
   - **Incident Response:** Azure maintains a skilled incident response team that is ready to react swiftly and effectively to any security incidents.
4. **Data Security:**
   - **Encryption:** Data within Azure data centres is encrypted at rest and in transit, using industry-standard protocols.
   - **Data Resilience:** Azure employs a variety of strategies to ensure data resilience, including redundant power supplies, backup generators, and network connections.
5. **Compliance and Certifications:**
   - Azure data centres comply with a range of international and industry-specific standards, such as ISO 27001, SOC 1, SOC 2, PCI DSS, and HIPAA.
   - Regular audits are conducted to ensure ongoing compliance with these standards.
6. **Infrastructure Management:**
   - **Hardware Security:** The hardware in Azure data centres is designed with security in mind, including features like Trusted Platform Modules (TPMs) and secure boot.
   - **Automated Management:** Azure employs sophisticated software for the automated management of resources, reducing the risk of human error.
7. **Redundancy and Reliability:**
   - Azure data centres are designed to be highly redundant and reliable, with measures in place to ensure uninterrupted power supply and network connectivity.

By integrating these various elements, Azure provides a secure and resilient environment for its global network of data centres, ensuring the integrity, confidentiality, and availability of customer data and services.

Principle 2.3: data encryption

Goals

Your data should be adequately protected from unauthorised access by parties with physical access to infrastructure, when considered alongside data at rest protections provided by encryption.

Service providers should encrypt all customer data at rest within the service, using an appropriate encryption algorithm and mode, as described below.

You should prefer a cloud provider that encrypts all data at rest by default, including any metadata derived from that data.

For this encryption, a symmetric encryption algorithm should be used in a mode of operation that provides both confidentiality (to prevent unauthorised reading of the data) and integrity (to prevent un-noticed tampering of the encrypted data).

Even a good algorithm will be vulnerable to attack if it's not used in a good mode of operation. So, both the algorithm and mode of operation used should be approved for general use. For example, an algorithm from NIST-SP-800-131A, and a suitable mode of operation from NIST-SP-800-38. At the time of writing, these include the symmetric algorithm AES, and the modes of operation GCM and XTS. You may see these described as AES-GCM or AES-XTS.

Principle 2.3: data encryption - Our comment

Data encryption in Microsoft Azure is a fundamental aspect of its security architecture, ensuring the confidentiality and integrity of data both at rest and in transit. Azure provides a range of encryption capabilities to protect data and help meet organisational compliance and security requirements. Here's an overview:

1. **Encryption at Rest:**
   - **Azure Storage Encryption:** Azure automatically encrypts data before storing it in Azure Blob Storage, File Storage, and Queue Storage, using Storage Service Encryption (SSE) with 256-bit Advanced Encryption Standard (AES) encryption.
   - **Azure Disk Encryption:** Azure offers disk encryption for virtual machines using BitLocker for Windows and DM-Crypt for Linux. This encryption helps protect and safeguard the data to meet organisational security and compliance commitments.
   - **Azure SQL Database Encryption:** Azure SQL Database uses Transparent Data Encryption (TDE) to encrypt database files at rest, helping protect against the threat of malicious activity.
2. **Encryption in Transit:**
   - **TLS/SSL Encryption:** Azure uses Transport Layer Security (TLS) and Secure Sockets Layer (SSL) to encrypt data in transit. This is the standard for ensuring that data remains private and integral while being transferred over the internet.
   - **End-to-End Encryption:** Customers can implement additional end-to-end encryption within their applications using application-level or database-level encryption techniques.
3. **Key Management:**
   - **Azure Key Vault:** Azure Key Vault is a centralised cloud service for storing application secrets and encryption keys. Key Vault helps streamline key management and maintain control over keys used for encrypting data.
   - **Customer-Managed Keys:** Azure offers the option for customers to manage their own encryption keys, which can be stored in Azure Key Vault or in the customer's own HSM (Hardware Security Module). This allows customers to meet more stringent compliance requirements.
4. **Application-Specific Encryption:**
   - **Azure App Service:** Offers the ability to secure application data using TLS/SSL for data in transit and provides integration with Azure Key Vault for securing application secrets.
   - **Azure Cosmos DB:** Provides encryption at rest by default and allows for secure transmission of data over encrypted channels.
5. **Compliance and Standards:**
   - Azure encryption services comply with international and industry-specific compliance standards, such as ISO 27001, HIPAA, and PCI DSS.
6. **Encryption for Specialised Workloads:**
   - Azure provides encryption solutions for specialised workloads, like Azure Blockchain Service and Azure Confidential Computing. Confidential Computing, for instance, offers data encryption in use, meaning data is protected even during processing.

Azure's comprehensive encryption capabilities ensure that data is protected across all service layers and adheres to best practices in data security and compliance. The flexibility in key management and the integration of encryption services into a broad range of Azure offerings make it easier for organisations to secure their data in the cloud.

Principle 2.4: data sanitisation and equipment disposal

Goals

The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to your data. You should be confident that:

- your data is erased when resources are moved or re-provisioned, or when you request it to be erased
- storage media which has held your data is sanitised or securely destroyed at the end of its life

Principle 2.4: data sanitisation and equipment disposal - Our comment

Data sanitisation and equipment disposal are important aspects of data security, especially in cloud environments like Microsoft Azure. These processes involve the removal, deletion, or destruction of data to prevent unauthorised access to sensitive information, especially when hardware is retired or repurposed. Here's how these aspects are typically handled in Azure:

1. **Data Sanitisation:**
   - **Data Deletion:** When a customer deletes data or terminates a service, Azure follows strict procedures to permanently delete the data. This involves overwriting the data to ensure it cannot be recovered.
   - **Automated Processes:** Azure uses automated processes to help ensure that data is securely deleted and cannot be recovered once a customer has deleted it from their environment. This includes data stored in virtual machines, databases, and storage accounts.
2. **Equipment Disposal:**
   - **Physical Hardware Destruction:** When physical hardware used in Azure data centres reaches the end of its life, Microsoft ensures that it is disposed of securely. This may involve physical destruction, such as shredding of hard disks and other storage media.
   - **Certified Disposal Processes:** Microsoft follows environmentally responsible processes for disposing of old hardware. This often involves partnering with certified vendors who specialise in the secure disposal of electronic waste.
3. **Data Centre Operations:**
   - **Regular Audits:** Regular audits of data centre operations ensure adherence to security, data sanitisation, and equipment disposal policies.
   - **Compliance with Standards:** The processes for data sanitisation and equipment disposal comply with various industry standards and regulations, ensuring that sensitive data is irrecoverable once the hardware is retired.
4. **Data at Rest:**
   - **Encryption:** Azure encrypts data at rest, which adds an additional layer of security. Even if the physical media were to be improperly disposed of, the data would remain encrypted and, therefore, largely inaccessible.
5. **Documentation and Policies:**
   - **Transparency:** Microsoft provides documentation on their data deletion and hardware disposal practices, offering transparency to customers about how their data is handled and protected throughout its lifecycle.
6. **Customer Responsibilities:**
   - **Data Management:** Customers are responsible for managing the lifecycle of their data in Azure, including ensuring that data is deleted as per their own data management policies.
   - **Data Backup:** Before deletion or termination of services, customers should ensure that they have backed up any necessary data.
7. **Environmental Considerations:**
   - **Sustainable Practices:** Microsoft is committed to sustainable practices in its data centre operations, including the recycling and disposal of hardware.

In summary, data sanitisation and equipment disposal in Azure are handled with a high degree of security and responsibility, ensuring that customer data is protected even after it is no longer in use. These practices are integral to maintaining the overall security and trustworthiness of cloud services.

Principle 2.5: physical resilience and availability

Goals

You should be sufficiently confident that:

- the availability commitments of the service, including their ability to recover from outages, meets your business needs
- you understand whether the provider's resilience processes have any implications for data residency
- you can protect your data from ransomware attacks

You should prefer a service that makes it easy to determine whether your configuration of a cloud service (including the use of multiple regions or availability zones) will provide the level of automatic failover and redundancy that you expect.

Principle 2.5: physical resilience and availability - Our comment

Physical resilience and availability are key components of Microsoft Azure's infrastructure, ensuring that services remain operational and accessible even in the face of hardware failures, natural disasters, and other disruptions. Here's how Azure achieves this:

1. **Global Network of Data Centres:**
   - **Geographical Distribution:** Azure operates a vast network of data centres across multiple geographic regions worldwide. This global presence not only brings services closer to users for reduced latency but also provides geographical redundancy.
   - **Regional Pairs:** Azure regions are often paired to provide redundancy. In the event of a major incident in one region, its paired region can provide failover capability.
2. **Data Centre Design and Construction:**
   - **Resilient Infrastructure:** Azure data centres are built with redundant power, cooling, and networking systems to ensure continuous operation.
   - **High Availability:** The infrastructure is designed for high availability, with components that can be serviced or replaced without impacting services.
3. **Redundancy and Replication:**
   - **Data Replication:** Azure provides multiple options for data replication, such as Locally Redundant Storage (LRS), Zone-Redundant Storage (ZRS), and Geo-Redundant Storage (GRS) to ensure data durability and high availability.
   - **Application Redundancy:** Azure encourages the design of fault-tolerant and redundant applications through features like Azure Load Balancer and Azure Traffic Manager.
4. **Power and Cooling Systems:**
   - **Redundant Power Supplies:** Azure data centres have backup power supplies, including generators and batteries, to ensure continuous operation during power outages.
   - **Efficient Cooling Systems:** Advanced cooling systems maintain optimal operating temperatures for data centre equipment.
5. **Network Resilience:**
   - **Redundant Network Connectivity:** Azure provides multiple network connections to and within data centres to prevent single points of failure.
   - **DDoS Protection:** Built-in Distributed Denial of Service (DDoS) protection defends against external attacks that can cause downtime.
6. **Disaster Recovery and Business Continuity:**
   - **Azure Site Recovery:** This service enables businesses to maintain business continuity by automating the replication of Azure Virtual Machines to different Azure regions.
   - **Backup Services:** Azure Backup provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud.
7. **Monitoring and Maintenance:**
   - **Proactive Monitoring:** Azure uses advanced monitoring systems to continuously track the health and performance of infrastructure and services.
   - **Regular Maintenance:** Regular updates and maintenance are conducted to ensure the infrastructure remains robust and secure.
8. **Compliance and Certifications:**
   - **Industry Standards:** Azure complies with key international and industry-specific standards, ensuring that its infrastructure meets stringent requirements for security and resilience.
9. **Environmental Controls:**
   - **Protection Against Natural Disasters:** Azure data centres are equipped with measures to protect against natural disasters, including elevated buildings and flood controls.

By leveraging these strategies, Azure ensures that its physical infrastructure is resilient and that services remain highly available, providing customers with a reliable and secure cloud computing environment.

Principle 3: Separation between customers

Separation techniques ensure a customer's service can't access or affect the service (or data) of another.

You rely on security boundaries implemented by your cloud provider to ensure that:

- you can control who can access your data, and how
- the service is robust enough to defend against another customer having malicious code in their instance of the service

Large cloud services, such as cloud platforms, may offer many different services. These services might each take a different approach to separation.

Goals

Your provider should be able to explain how they have implemented security separation within their service. This includes the security boundaries in:

- compute (such as containerisation, Functions-as-a-Service, and IaaS)
- storage
- data flows and networking

If a SaaS or PaaS service is built on top of other PaaS or IaaS services (such as in a third-party cloud), your provider should explain which separation properties are inherited from the underlying components and infrastructure.

You should be confident that for each service you use, you know which separation mechanisms are used and that they are appropriate for your needs.

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-3-separation-between-customers

Principle 3: Separation between customers - Our comment

Separation between customers, often referred to as multi-tenancy, is a fundamental aspect of cloud computing, including Microsoft Azure. This concept involves securely isolating data, applications, and resources belonging to different customers (tenants) who use shared infrastructure. Azure employs several mechanisms to ensure this separation and maintain privacy and security for each tenant. Here's an overview:

1. **Network Isolation:**
   - **Virtual Networks:** Azure Virtual Network (VNet) allows customers to create isolated networks within Azure. Each VNet is separate from other VNets and provides a private IP address space.
   - **Subnets and Network Security Groups (NSGs):** Within VNets, customers can further segregate their network into subnets and use NSGs to control inbound and outbound network traffic to and from resources.
2. **Identity and Access Management:**
   - **Azure Active Directory (AAD):** Azure uses AAD for identity services. It ensures that each customer's identity services are isolated and that one customer cannot access another's identities or resources.
   - **Role-Based Access Control (RBAC):** RBAC allows customers to define precise access permissions for users and services, ensuring they have access only to the resources they are supposed to.
3. **Storage Isolation:**
   - **Encrypted Storage:** Data in Azure Storage is encrypted, ensuring that one customer's data is not accessible to another.
   - **Access Controls:** Azure provides fine-grained access controls for storage resources, such as Storage Account Keys and Shared Access Signatures (SAS), to control access to storage accounts.
4. **Compute Isolation:**
   - **Virtual Machines (VMs):** VMs are isolated from one another at the hypervisor level. Azure uses a hypervisor to enforce memory and process separation between VMs.
   - **App Service Environments (ASEs):** For even greater isolation, Azure offers ASEs, which provide fully isolated and dedicated environments for securely running App Service apps.
5. **Database Isolation:**
   - **SQL Database:** Azure SQL Database uses a multi-tenant architecture that isolates each database at the application and database level.
   - **Managed Instance:** For higher isolation requirements, Azure SQL Database Managed Instance provides an isolated SQL environment within a private VNet.
6. **Resource Management:**
   - **Azure Resource Manager (ARM):** ARM is a layer that enables management and deployment of resources in Azure. It provides isolation and management of resources in a secure and compliant manner.
7. **Monitoring and Compliance:**
   - **Activity Logs and Monitoring Tools:** Azure provides activity logs and monitoring tools that allow customers to monitor their resources independently.
8. **Physical Isolation Option:**
   - For customers with the highest security needs, Azure offers physically isolated data centre options through services like Azure Dedicated Host and Azure Stack.

These mechanisms collectively ensure that while Azure's infrastructure is shared among multiple customers, each customer's data, applications, and services remain isolated and protected. This approach is crucial for maintaining security and privacy in the cloud, and for meeting regulatory and compliance requirements.

Principle 4: Governance framework

A governance framework is vital to co-ordinate and direct the management of the service.

An effective governance framework will ensure that procedural, personnel, physical and technical controls continue to work through the lifetime of a service. It should also respond to changes in the service, technological developments, and the appearance of new threats.

Goals

You should be confident that the service has a governance framework and processes which are appropriate for your intended use.

You should look for good governance practices, including:

- A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This person will typically have the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer'.
- A documented framework for security governance and risk management, with policies governing key aspects of information security, relevant to the service.
- Security and information security are part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board will be kept informed of security and information risk.
- Processes to identify and ensure compliance with applicable legal and regulatory requirements.

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-4-governance-framework

Principle 4: Governance framework - Our comment

Governance in Microsoft Azure refers to the mechanisms, processes, and policies that help ensure effective management, security, compliance, and operational efficiency of cloud resources. Azure provides a comprehensive framework for governance that enables organisations to maintain control over their cloud environments. This framework encompasses several key components:

1. **Azure Policy:**
   - **Policy Enforcement:** Azure Policy helps in enforcing organisational standards and assessing compliance at scale. It allows you to create, assign, and manage policies that enforce rules over your resources, ensuring they stay compliant with corporate standards and service level agreements (SLAs).
   - **Compliance Assessment:** It continuously monitors resource compliance and can automatically remediate non-compliant resources.
2. **Azure Blueprints:**
   - **Template-Based Environments:** Azure Blueprints enable the creation of repeatable, pre-configured templates for setting up environments according to organisational standards. These blueprints can include role assignments, policy assignments, Azure Resource Manager templates, and Resource Groups.
   - **Version Control and Tracking:** Blueprints can be versioned and tracked, ensuring consistent application of environments across the organisation.
3. **Role-Based Access Control (RBAC):**
   - **Access Management:** RBAC in Azure provides fine-grained access management to Azure resources. It allows organisations to segregate duties within their team and grant only the amount of access to users that they need to perform their jobs.
   - **Built-In and Custom Roles:** Azure offers built-in roles and the ability to create custom roles, tailoring access to specific needs and requirements.
4. **Azure Management Groups:**
   - **Resource Hierarchy:** Management Groups provide a level of scope above subscriptions. You can organise subscriptions into containers called "management groups" and apply governance policies to these groups.
   - **Policy and Compliance Inheritance:** Policies applied at the management group level are inherited by all subscriptions within that management group.
5. **Cost Management and Analysis:**
   - **Budgets and Alerts:** Azure Cost Management provides tools for monitoring, controlling, and optimising cloud spend. You can set budgets and configure alerts to keep spending in check.
   - **Cost Analysis:** Detailed cost analysis tools help in understanding and managing cloud costs effectively.
6. **Resource Locks:**
   - **Protection Against Accidental Deletion/Modification:** Resource locks prevent accidental deletion or modification of critical Azure resources.
7. **Tags and Resource Organisation:**
   - **Resource Tagging:** Tags allow you to annotate resources with metadata. This is useful for organising resources, managing costs, and enforcing policy.
8. **Compliance and Regulatory Standards:**
   - **Compliance Dashboard:** Azure provides a compliance dashboard in Azure Security Centre to view the compliance status of the resources under Azure policies.
   - **Support for Regulatory Standards:** Azure aligns with various international and industry-specific compliance standards, providing tools and documentation to assist in meeting regulatory requirements.
9. **Monitoring and Auditing:**
   - **Azure Monitor and Azure Activity Log:** These tools provide data and insights to monitor the performance and health of your applications, infrastructure, and network.
10. **Azure Advisor:**
    - **Best Practices Guidance:** Azure Advisor provides personalised recommendations to optimise Azure resources for high availability, security, performance, and cost.

This governance framework helps organisations in Azure to enforce policies, ensure compliance, manage risks, optimise costs, and maintain operational excellence as they scale their cloud environments.

Principle 5: Operational security

Services must be operated and managed in a way to impede, detect or prevent attacks.

Good operational security should not require complex, bureaucratic, time consuming or expensive processes. The aspects to consider are:

1. Vulnerability management
2. Protective monitoring
3. Incident management
4. Configuration and change management

Principle 5.1: vulnerability management

Goals

Your provider should have a vulnerability management process in place to identify, triage and mitigate vulnerabilities in all components of the service that they are responsible for.

Note: For more information about how to assess and prioritise vulnerabilities, please refer to the NCSC's Vulnerability Management guidance.

You should be confident that:

- you know your service provider's timescales for deploying security updates and other mitigations, and are happy with them
- your provider takes responsibility for applying security updates to all software and hardware, including where they rely on external dependencies (or a third-party supply chain)
- potential new threats, vulnerabilities or exploitation techniques that could affect your service are proactively assessed and corrective action is taken

You should prefer a provider that:

- attempts to identify vulnerabilities in off-the-shelf components used by the service that you have deployed on top of the cloud platform
- automatically applies mitigations

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-5-operational-security

Principle 5.1: vulnerability management - Our comment

Vulnerability management in Microsoft Azure is a critical component of the cloud security framework. It involves identifying, assessing, mitigating, and reporting on security vulnerabilities within the Azure environment. Microsoft employs a range of tools and practices to manage vulnerabilities effectively, ensuring that the Azure infrastructure and customer data remain secure. Here's an overview:

1. **Regular Vulnerability Scanning:**
   - **Automated Scanning:** Azure continuously scans for vulnerabilities within its infrastructure. This includes scanning for common vulnerabilities in the operating systems, services, and applications that are part of the Azure platform.
   - **Integration with Security Tools:** Azure integrates with advanced security tools that can identify potential vulnerabilities in customer-deployed applications and resources.
2. **Patch Management:**
   - **Automated Patching:** Azure automatically applies security patches to its managed services. For Infrastructure as a Service (IaaS) offerings like Azure Virtual Machines, customers can use Azure Update Management to automate the patching process.
   - **Regular Updates:** Microsoft ensures that all software running in Azure data centres is up to date with the latest security patches.
3. **Threat Intelligence:**
   - **Microsoft Security Intelligence:** Azure leverages the extensive threat intelligence gathered by Microsoft, which helps in proactively identifying and responding to emerging threats and vulnerabilities.
   - **Azure Security Centre:** This provides advanced threat protection and security health monitoring, which includes assessing for vulnerabilities.
4. **Risk Assessment:**
   - **Vulnerability Assessment Tools:** Azure offers built-in vulnerability assessment tools for virtual machines and container workloads. These tools help customers identify and remediate vulnerabilities.
   - **Security Scores and Recommendations:** Azure Security Centre provides security scores and actionable recommendations, helping customers prioritise and address potential vulnerabilities.
5. **Third-Party Security Solutions:**
   - **Marketplace Integrations:** Azure integrates with a variety of third-party security solutions available through the Azure Marketplace, offering customers additional options for vulnerability assessment and management.
6. **Incident Response and Remediation:**
   - **Rapid Response:** Azure has a dedicated incident response team that quickly addresses vulnerabilities and security incidents.
   - **Remediation Guidance:** In case of a vulnerability or breach, Azure provides guidance and tools for rapid remediation.
7. **Communication and Transparency:**
   - **Security Advisories and Updates:** Microsoft communicates regularly with customers about security issues, vulnerabilities, and patches through advisories and Azure Service Health notifications.
   - **Compliance Reports and Documentation:** Azure provides detailed compliance reports and documentation to help customers understand Microsoft's vulnerability management processes.
8. **Compliance and Auditing:**
   - **Regular Audits:** Azure undergoes regular third-party audits to ensure compliance with various industry standards, and the results of these audits are available to customers.
9. **Customer Responsibility:**
   - **Shared Responsibility Model:** While Microsoft manages the security of the Azure platform, customers are responsible for securing their applications and data in Azure. This includes regular vulnerability scanning, patch management, and following best practices.

Vulnerability management in Azure is a continuous and proactive process. Microsoft's comprehensive approach to identifying, mitigating, and managing vulnerabilities, combined with the tools and practices provided to customers, helps ensure a secure cloud environment.

5.2 Protective monitoring

Goals

Your provider should monitor for attacks, misuse and malfunction to help it detect successful and unsuccessful attacks against the service as a whole, or the parts of the service that it runs on your behalf. This will allow it to quickly respond to potential compromises of your environment and data.

You should be sufficiently confident that:

- the service generates adequate audit events to support effective identification of suspicious activity
- the collected events are analysed to identify potential compromises or inappropriate use of the cloud service
- the service provider takes prompt and appropriate action to address incidents

5.2 Protective monitoring - Our comment

Protective monitoring in Microsoft Azure refers to the practices and technologies used to continuously observe, detect, and respond to potential security threats and vulnerabilities. This proactive approach is essential for maintaining the security and integrity of cloud resources and data. Azure employs a comprehensive set of tools and services for effective protective monitoring:

1. **Azure Security Centre:**
   - **Unified Security Management:** Azure Security Centre offers a centralised view of the security posture of all Azure resources. It continuously monitors these resources for security issues and provides actionable recommendations to improve security.
   - **Advanced Threat Protection:** It includes advanced threat detection capabilities, leveraging analytics and Microsoft's global threat intelligence to identify and respond to potential threats quickly.
2. **Azure Monitor:**
   - **Real-Time Monitoring:** Azure Monitor collects and analyzes data from Azure resources, providing insights into performance, operations, and health. This data includes metrics, logs, and other telemetry.
   - **Alerting and Diagnostics:** Users can set up alerts based on specific metrics or log queries to get notified of potential issues. Diagnostic settings allow the routing of logs and metrics to various destinations for deeper analysis.
3. **Azure Sentinel:**
   - **Cloud-Native SIEM:** Azure Sentinel is a scalable, cloud-native SIEM (Security Information and Event Management) solution that provides intelligent security analytics across the enterprise. It uses AI to analyze large volumes of data across the enterprise.
   - **Incident Detection and Response:** Sentinel helps in detecting, investigating, and responding to security incidents. It provides sophisticated investigation tools and integrates with other Azure services for automated response.
4. **Log Analytics:**
   - **Data Collection and Analysis:** Part of Azure Monitor, Log Analytics collects and analyzes log data from various Azure resources. This analysis helps in identifying anomalies, trends, and potential security threats.
   - **Query and Visualisation:** Users can query the collected data using Kusto Query Language (KQL) and visualise results for better insights.
5. **Network Security:**
   - **Azure Firewall and Network Security Groups (NSGs):** These provide essential network-level protection and monitoring, allowing control over inbound and outbound traffic based on defined security rules.
   - **Azure DDoS Protection:** This service provides monitoring and protection against distributed denial-of-service (DDoS) attacks.
6. **Identity and Access Management:**
   - **Azure Active Directory (AAD):** AAD provides monitoring and reporting features for identity and access, including sign-in logs, audit logs, and risk detection.
   - **Conditional Access and Multi-Factor Authentication (MFA):** These features help monitor and secure user access to Azure resources.
7. **Compliance and Reporting:**
   - **Regulatory Compliance Dashboard:** Azure Security Centre includes a compliance dashboard that assesses the compliance of Azure resources against various regulatory standards and provides recommendations for compliance improvement.
8. **Integration with Third-Party Solutions:**
   - **Azure Marketplace:** Azure integrates with a wide range of third-party security and monitoring tools available in the Azure Marketplace, offering extended capabilities.

Protective monitoring in Azure involves a combination of automated tools, advanced analytics, and integration with global threat intelligence. This comprehensive approach enables rapid detection, analysis, and response to potential security threats, ensuring a robust security posture for Azure environments.

5.3 Incident management

Goals

Your cloud provider should have pre-planned incident management processes in place, to make it more likely that effective and prompt decisions are made when incidents occur. The processes needn't be complex or require large amounts of description, but good incident management will minimise the impact to users of security, reliability and environmental issues with a service.

You should have confidence that:

- incident management processes are in place for the service and are actively deployed in response to security incidents
- pre-defined processes are in place for responding to common types of incident and attack
- a defined process and contact route exist for customers and external entities to report security incidents and vulnerabilities
- the service provider will inform you if they detect a security incident that affects your data in an acceptable agreed timescale

5.3 Incident management - Our comment

Incident management in Microsoft Azure refers to the processes and tools used to detect, respond to, and resolve security incidents within the Azure environment. Microsoft has established robust mechanisms to handle incidents promptly and efficiently, ensuring minimal impact on services and customers. Here's an overview of how incident management is implemented in Azure:

1. **Incident Detection:**
   - **Azure Security Center:** Provides advanced threat protection that continuously monitors Azure resources for suspicious activities and security threats.
   - **Azure Sentinel:** Azure's cloud-native SIEM (Security Information and Event Management) system collects and analyzes large volumes of data across the enterprise, using advanced analytics and machine learning to identify potential security incidents.
2. **Alerting and Notification:**
   - **Automated Alerts:** Both Azure Security Center and Azure Sentinel are capable of generating automated alerts when potential security incidents are detected.
   - **Customizable Alert Rules:** Customers can create custom alert rules based on specific conditions, ensuring that they are promptly notified of incidents that matter most to their environment.
3. **Response Coordination:**
   - **Incident Response Team:** Microsoft has a dedicated incident response team that is responsible for managing security incidents within Azure. This team coordinates the response efforts, including investigation and remediation activities.
   - **Customer Communication:** In the event of a significant incident, Microsoft communicates with affected customers, providing information about the incident and guidance on mitigation measures.
4. **Investigation and Analysis:**
   - **Forensic Analysis:** Tools and processes are in place for conducting forensic analysis to understand the scope, impact, and root cause of incidents.
   - **Log Analytics:** Azure provides extensive logging and analytics capabilities, allowing customers to conduct their own investigations into incidents within their environments.
5. **Remediation and Recovery:**
   - **Guided Remediation:** Azure Security Center provides recommendations and guidance for remediation of identified security issues.
   - **Recovery Services:** Azure offers services such as Azure Site Recovery and Azure Backup to assist in the recovery process in the event of an incident.
6. **Post-Incident Review and Learning:**
   - **Lessons Learned:** After an incident is resolved, a post-incident review is conducted to gather lessons learned and to improve future response efforts.
   - **Continuous Improvement: I**nsights gained from incidents are used to continuously improve Azure's security posture and incident response capabilities.
7. **Compliance and Reporting:**
   - **Regulatory Compliance:** Azure ensures that incident management processes are compliant with various regulatory requirements, and provides necessary reporting to assist customers in their compliance efforts.
   - **Audit Trails:** Azure maintains audit trails and logs that are critical for compliance and post-incident analysis.
8. **Customer Roles and Responsibilities:**
   - **Shared Responsibility Model:** Customers are responsible for managing the security of their applications and data on Azure. This includes configuring alert rules, monitoring their resources, and responding to incidents within their environments.

By implementing these practices, Azure ensures a comprehensive approach to incident management, enabling quick detection, efficient response, and effective resolution of security incidents, thereby maintaining the trust and integrity of its cloud services.

5.4 Configuration and change management

Goals

Your provider should know what assets make up their service along with their configurations and dependencies, allowing them to identify and manage changes which could affect the security of the service and fully mitigate vulnerabilities that they are aware of.

You should be confident that:

- the status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime
- changes to the service are assessed for potential security impact, then managed and tracked through to completion
- unauthorised changes to the deployed service components and their configuration will be detected and prevented
- the cloud provider will give you appropriate notice before making changes that affect how you use the service or your ability to use the service

You should prefer a cloud provider that:

- implements all technical change automatically and consistently across their infrastructure

5.4 Configuration and change management - Our comment

Configuration and change management in Microsoft Azure involve processes and tools designed to help manage and track changes to Azure resources and configurations, ensuring that these changes are made in a controlled and secure manner. Effective configuration and change management is crucial for maintaining the stability, security, and compliance of cloud environments. Here's how Azure facilitates this:

1. **Azure Resource Manager (ARM):**
   - **Resource Management:** ARM is a service that enables you to manage and deploy Azure resources. It provides a consistent management layer for tasks such as resource deployment, update, and deletion.
   - **Templates for Deployment:** ARM templates allow you to define and deploy infrastructure as code, which promotes consistent and repeatable deployments.
2. **Azure Policy:**
   - **Policy Enforcement:** Azure Policy helps you define and enforce policies that ensure your resources remain compliant with organizational standards and SLAs.
   - **Compliance Assessment:** It continuously assesses your resources for compliance with these policies and can automatically remediate non-compliant resources.
3. **Azure Blueprints:**
   - **Standardized Environments:** Azure Blueprints enable you to create and deploy standardized environments with a set of predefined resources, policies, and role assignments.
4. **Change Tracking and Inventory:**
   - **Monitoring Changes:** Azure provides tools for tracking changes and managing inventory across Azure resources. This includes monitoring changes to configurations and file integrity.
5. **Version Control Integration:**
   - **Integration with DevOps Tools:** Azure integrates with version control systems like Azure Repos or GitHub, facilitating version control for your infrastructure as code and configurations.
6. **Role-Based Access Control (RBAC):**
   - **Access Control:** RBAC controls who has access to Azure resources and what actions they can perform, which is vital for managing changes securely.
7. **Monitoring and Auditing:**
   - **Azure Monitor and Azure Activity Log:** These services provide insights into operational data, monitoring the performance and health of resources. The Activity Log records all write operations (PUT, POST, DELETE) performed on your resources.
   - **Log Analytics:** Allows you to query and analyze the logs collected from your Azure resources.
8. **Azure Automation:**
   - **Automated Configuration Management:** Azure Automation delivers a cloud-based automation service for automating manual, long-running, error-prone, and frequently repeated tasks.
9. **Compliance and Standards:**
   - **Regulatory Compliance:** Azure ensures that configuration and change management processes are compliant with various regulatory requirements.
   - **Reporting and Documentation:** Azure provides detailed documentation and reporting capabilities to support compliance and auditing processes.
10. **Azure DevOps Services:**
    - **Continuous Integration/Continuous Deployment (CI/CD):** Azure DevOps Services provide tools for implementing CI/CD pipelines, allowing you to automate the build, testing, and deployment of applications.

By leveraging these tools and practices, organizations can manage changes in their Azure environment effectively, ensuring that configurations are consistent, compliant, and aligned with their business objectives and security requirements.

Principle 6: Personnel security

Audit and constrain the actions of service provider personnel.

Where service provider personnel have access to your data and systems, you need to have enough confidence in their trustworthiness, and the technical measures in place that audit and constrain the actions of those personnel.

Effective personnel controls should be a balance of:

- the provider demonstrating how they gain enough confidence in their people
- technical controls that minimise the likelihood and impact of accidental or malicious compromise by service provider personnel

Principle 6.1: people and security culture

The service provider should subject personnel to security screening and regular security training, appropriate to their role and privileges. Providers should make clear how they screen and manage personnel within privileged roles.

Goals

You should be confident that:

- the minimum number of people have access to your data, or could affect your use of the service
- the provider has implemented a positive security culture across their organisation
- the level of security screening conducted on service provider staff or contractors that have access to your data, or have the ability to affect your service, is appropriate

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-6-personnel-security

Principle 6.1: people and security culture - Our comment

The people and security culture surrounding Microsoft Azure is a fundamental aspect of its overall security posture. It encompasses the attitudes, behaviors, and practices of Microsoft's employees, contractors, and partners, all of whom play critical roles in maintaining and enhancing the security of Azure services. Here's an overview of how people and security culture are addressed when using Azure:

1. **Security-First Mindset:**
   - **Culture of Security:** Microsoft fosters a culture where security is a top priority. This is embedded in all aspects of the organisation, from the development of Azure services to their deployment and maintenance.
   - **Continuous Learning and Improvement:** Employees are encouraged to stay informed about the latest security trends and threats, fostering a culture of continuous learning and improvement in security practices.
2. **Employee Training and Awareness:**
   - **Regular Security Training:** All Microsoft employees, including those working on Azure, undergo regular security training. This training covers a range of topics, from basic security awareness to advanced topics for specialised roles.
   - **Phishing and Social Engineering Defense:** Employees are trained to recognise and respond to phishing attempts and social engineering tactics, which are common attack vectors.
3. **Role-Based Access and Least Privilege:**
   - **Access Controls:** Access to Azure's infrastructure and customer data is strictly controlled and based on the principle of least privilege. Employees are granted access only to the resources necessary for their job functions.
   - **Regular Access Reviews:** Microsoft conducts regular reviews of employee access rights to ensure that access privileges remain aligned with job requirements.
4. **Secure Development Lifecycle (SDL):**
   - **Incorporating Security in Development:** Azure services are developed following Microsoft's Secure Development Lifecycle, a framework that integrates security and privacy into software development.
   - **Security Testing and Code Reviews:** Regular security testing, including code reviews and vulnerability assessments, is part of the development process for Azure services.
5. **Incident Response Training:**
   - **Preparedness:** Microsoft ensures that employees are prepared to respond effectively to security incidents. This includes regular drills and training on incident response protocols.
   - **Clear Reporting Channels:** Employees have clear channels for reporting security incidents, anomalies, or vulnerabilities.
6. **Transparency and Trust:**
   - **Open Communication:** Microsoft values transparency and maintains open communication with its customers regarding security practices, incident reports, and compliance information.
   - **Customer Trust:** Building and maintaining customer trust is a key aspect of Microsoft's security culture, with a strong emphasis on protecting customer data and privacy.
7. **Community Engagement and Collaboration:**
   - **Security Research Community:** Microsoft collaborates with the broader security research community to stay ahead of emerging threats. They encourage responsible vulnerability disclosure and often engage with external security researchers.
8. **Compliance and Ethical Standards:**
   - **Adherence to Regulations:** Microsoft adheres to various international and industry-specific security standards and regulations, ensuring that their practices meet high ethical and legal standards.
9. **Promoting a Secure Ecosystem:**
   - **Partner and Vendor Security:** Microsoft extends its security culture to its partners and vendors, requiring them to adhere to strict security standards and practices.

This combination of a strong security culture, continuous employee training, adherence to best practices, and an emphasis on ethical and legal compliance helps ensure that Azure remains a secure and trustworthy platform for its users.

Principle 6.2: technical controls for service administration

Personnel security should combine background checks and procedural controls with technical measures designed to detect and minimise the impact of a malicious insider.

Goals

You should be confident that:

- an administrator accessing your data, or making changes that affect your use of the service, will be reliably logged and monitored
- you will be alerted if the provider's personnel perform an action on the cloud service that could (accidentally or otherwise) expose them to your data

You should prefer a cloud provider that employs technical controls to reduce the likelihood of accidental or malicious compromise by service provider personnel.

Controls should include:

- administrators and privileged users are only given minimal administrative capabilities temporarily, in response to a specific issue (additional privileges should be requested when necessary)
- requests for additional privileges are tied either to a customer support ticket, or an internal change request
- access to systems or interfaces that could provide access to customer data is only granted if the customer has given explicit time-limited permission for that access (this applies on a case-by-case basis)

Principle 6.2: technical controls for service administration - Our comment

Technical controls for service administration in Microsoft Azure are designed to ensure secure and efficient management of Azure services. These controls help organisations enforce security policies, manage resource configurations, and protect against unauthorised access or changes to their Azure environment. Here's an overview of the key technical controls:

1. **Role-Based Access Control (RBAC):**
   - **Access Management:** RBAC is used to assign permissions to users, groups, and applications at a fine-grained level. It ensures that administrators have only the access they need to perform their tasks.
   - **Built-In and Custom Roles:** Azure provides built-in roles like Owner, Contributor, Reader, and more, and also allows the creation of custom roles for specific needs.
2. **Azure Policy:**
   - **Policy Enforcement:** Azure Policy helps enforce organisational standards and assess compliance at scale. It allows the creation and assignment of policies that enforce rules for Azure resources, ensuring they stay compliant with corporate standards and SLAs.
   - **Compliance Assessment:** It continuously monitors resource compliance with the assigned policies.
3. **Azure Blueprints:**
   - **Standardised Environments:** Azure Blueprints enable the creation of repeatable sets of Azure resources that adhere to organisational standards. They package role assignments, policy assignments, ARM templates, and Resource Groups.
4. **Azure Resource Manager (ARM):**
   - **Resource Management and Deployment:** ARM provides a management layer that enables you to create, update, and delete resources in your Azure account. It uses JSON templates for the consistent deployment of Azure resources.
5. **Azure Active Directory (AAD):**
   - **Identity Services:** AAD provides identity services that support multi-factor authentication (MFA) and conditional access policies, enhancing the security of administrative access.
   - **Integration with Azure Services:** AAD integrates with various Azure services to manage identities and access to resources.
6. **Monitoring and Logging:**
   - **Azure Monitor and Azure Activity Log:** These services provide data and insights to monitor the performance and health of applications, infrastructure, and network, and track administrative operations.
   - **Log Analytics:** It helps in collecting, analyzing, and acting on telemetry data from Azure and on-premises environments.
7. **Network Security:**
   - **Network Security Groups (NSGs) and Azure Firewall:** These provide network-level filtering to control inbound and outbound traffic to Azure resources and subnets.
   - **Virtual Network (VNet) and Subnet Design:** Proper design of VNets and subnets ensures secure segmentation of the Azure environment.
8. **Encryption and Key Management:**
   - **Azure Key Vault:** Used for managing cryptographic keys and secrets used by cloud applications and services. It helps in protecting encryption keys and secrets like certificates, connection strings, and passwords.
9. **Automation for Compliance and Remediation:**
   - **Azure Automation:** This service helps in automating repeated tasks and processes, ensuring compliance with desired configurations and reducing the risk of human error.
10. **Privileged Identity Management (PIM):**
    - **Just-In-Time Access:** PIM in Azure AD provides time-bound and approval-based role activation to minimise the number of people who have persistent access to sensitive resources.

These technical controls collectively contribute to a secure and efficient administrative framework, enabling organisations to manage their Azure services effectively while maintaining compliance with security best practices and organisational policies.

Principle 7: Secure development

Cloud services should be designed, developed and deployed in a way that minimises and mitigates threats to their security.

Cloud services which aren't designed, developed and deployed in a secure way may be vulnerable to security issues which could compromise your data, cause loss of service, or enable other malicious activity.

Goals

You should be sufficiently confident that:

- the provider uses a software development lifecycle in line with our secure software development and deployment guidance, at a standard appropriate for the sensitivity of your data
- the provider has built a culture of secure development, including secure development training, code review of all deployed changes, and curation of well-understood libraries for solving security-critical problems
- the provider automates the integration and deployment pipeline used to deliver their cloud services, to enforce security, consistency, and a detailed audit trail
- the provider clearly separates their production environment from testing or development environments
- the provider risk-manages the supply chain of internal and third-party software libraries used in their code, only using supported external software
- the provider monitors the external software's security advisories and pulls in any security fixes promptly
- configuration and secrets management processes are in place to ensure the integrity of the cloud service throughout development, testing and deployment
- the provider maintains their services over time and responds to new and evolving threats

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-7-secure-development

Principle 7: Secure development - Our comment

Secure development in Microsoft Azure encompasses a comprehensive set of practices, tools, and guidelines designed to ensure that applications and services built on Azure are secure by design. Microsoft employs a security-focused development lifecycle and provides Azure users with the tools and resources needed to build secure applications. Here's an overview:

1. **Microsoft's Secure Development Lifecycle (SDL):**
   - **Integration of Security in Development:** SDL is Microsoft's industry-leading security process, which integrates security and privacy into software development. It includes security requirements analysis, design, implementation, verification, release, and response.
   - **Security Training for Developers:** Developers receive training in secure coding practices, common vulnerabilities and their mitigations, and how to build security into the software development lifecycle.
2. **Azure DevOps Security:**
   - **Secure DevOps Kit for Azure (AzSK):** This kit includes tools and practices for securely developing applications in Azure. It provides scripts, tools, extensions, and automation to ensure continuous security assurance.
   - **Automated Security Testing:** Azure DevOps supports the integration of automated security testing tools into the CI/CD pipeline, such as static application security testing (SAST) and dynamic application security testing (DAST).
3. **Application Security:**
   - **Application Insights and Azure Monitor:** These tools help in monitoring applications for security and performance issues.
   - **Web Application Firewall (WAF):** Azure provides a WAF that can be deployed with Azure Application Gateway to protect web apps from common web vulnerabilities and attacks.
4. **Identity and Access Management:**
   - **Azure Active Directory (AAD):** AAD provides robust identity services, ensuring secure authentication and authorisation for applications.
   - **Role-Based Access Control (RBAC):** RBAC helps in managing who has access to Azure resources, what they can do with those resources, and what areas they have access to.
5. **Data Protection and Encryption:**
   - **Azure Key Vault:** Used to safeguard cryptographic keys and secrets used by cloud applications and services.
   - **Encryption:** Azure supports encryption of data in transit and at rest, providing tools and best practices for implementing encryption.
6. **Network Security:**
   - **Virtual Networks (VNets) and Network Security Groups (NSGs):** These provide network isolation and protection, ensuring that applications are shielded from unauthorised network access.
   - **Private Link:** Azure Private Link provides private connectivity to Azure services, reducing exposure to the public internet.
7. **Threat Protection and Monitoring:**
   - **Azure Security Centre:** Offers advanced threat protection and security health monitoring, which includes assessing for vulnerabilities.
   - **Azure Sentinel:** A cloud-native SIEM solution that provides intelligent security analytics across the enterprise.
8. **Compliance and Standards:**
   - **Regulatory Compliance:** Azure complies with key international and industry-specific standards and offers tools to help users ensure their applications are compliant.
9. **Security Best Practices and Guidance:**
   - **Azure Architecture Centre:** Provides best practices and architectural guidance, including security considerations for application development.
10. **Third-Party Security Solutions:**
    - **Azure Marketplace:** Offers a variety of third-party security tools and services that can be integrated into Azure applications for enhanced security.

By utilising these secure development practices and tools, organisations can build and deploy applications on Azure that are secure, resilient, and compliant with industry standards. Microsoft's commitment to security in the cloud ecosystem ensures a robust foundation for developing secure cloud applications.

Principle 8: Supply chain security

Goals

You should be sufficiently confident that you understand:

- how your data is shared with (or made accessible to) third party suppliers and their supply chains, including the circumstances under which that data is shared
- which customer data, and metadata derived from that data, is shared with, or made accessible to third party supplies and their supply chains
- how the service provider's hardware and software procurement processes place security requirements on third party suppliers
- how the service provider manages security risks from third party suppliers
- how the service provider manages the conformance of their suppliers with security requirements

These concepts are covered in more detail in the NCSC's Supply chain guidance.

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-8-supply-chain-security

Principle 8: Supply chain security - Our comment

Supply chain security in Microsoft Azure is a critical component of its overall security strategy, addressing the risks associated with the hardware, software, and services that make up the cloud infrastructure. Microsoft takes a comprehensive approach to ensure the integrity and security of its supply chain, thereby protecting Azure services from potential vulnerabilities and threats that could arise from third-party components. Here's how supply chain security is managed in Azure:

1. **Vendor Selection and Management:**
   - **Rigorous Vetting Process:** Microsoft carefully selects and vets vendors and suppliers, assessing their security practices and compliance with industry standards.
   - **Ongoing Monitoring:** Continuous monitoring and auditing of suppliers ensure they adhere to contractual security obligations and best practices.
2. **Secure Hardware Procurement:**
   - **Trusted Hardware Sources:** Hardware components are sourced from trusted suppliers. Microsoft ensures the integrity of hardware used in Azure data centres.
   - **Hardware Security:** Use of hardware that includes security features like Trusted Platform Module (TPM) chips, which provide hardware-based security functions.
3. **Software Supply Chain Security:**
   - **Secure Software Development:** Microsoft follows its Secure Development Lifecycle (SDL) for all software development, including third-party software integrated into Azure.
   - **Third-Party Software Assessment:** Regular security assessments and code reviews of third-party software are conducted to identify and mitigate potential vulnerabilities.
4. **Risk Management in Procurement:**
   - **Contractual Requirements:** Contracts with suppliers include strict security requirements. Microsoft mandates compliance with these requirements for all components of the Azure supply chain.
   - **Supply Chain Risk Management (SCRM):** Microsoft employs a comprehensive SCRM process to identify, assess, and mitigate risks throughout the supply chain.
5. **Physical Supply Chain Security:**
   - **Data Centre Security:** Azure data centres are designed with multiple layers of physical security, including strict access controls and 24/7 monitoring, to protect against unauthorised access and tampering.
   - **Secure Transportation and Handling:** Secure logistics practices are followed for the transportation and handling of hardware and other critical components.
6. **Transparency and Compliance:**
   - **Regulatory Compliance:** Azure's supply chain adheres to global and regional compliance standards. Microsoft provides transparency into its compliance with various regulatory requirements.
   - **Audits and Certifications:** Regular third-party audits are conducted to certify the security and compliance of Azure's supply chain.
7. **Incident Response and Continuity:**
   - **Supply Chain Incident Response:** Microsoft has processes in place for responding to supply chain incidents, including a coordinated response for addressing vulnerabilities and breaches.
   - **Business Continuity Planning:** Strategies are in place to ensure continuity of service in the event of a supply chain disruption.
8. **Supplier Collaboration and Improvement:**
   - **Collaborative Security Efforts:** Microsoft collaborates with suppliers to improve security standards and practices across the supply chain.
   - **Supplier Development Programs:** Programs aimed at enhancing the security capabilities of suppliers are part of the overall strategy.
9. **Cybersecurity and Threat Intelligence:**
   - **Threat Monitoring and Intelligence Sharing:** Microsoft monitors for cybersecurity threats that may impact the supply chain and shares intelligence with suppliers and partners.

By implementing these comprehensive measures, Microsoft Azure ensures that its supply chain remains secure, resilient, and reliable, mitigating risks that could impact the security and integrity of its cloud services.

Principle 9: Secure user management

Providers should make tools available to securely manage your use of their service.

Your provider should make the tools available for you to securely manage your access to their service, preventing unauthorised access and alteration of your resources, applications and data.

Goals

You should be sufficiently confident that:

- there is a single, well-defined user account model
- you understand the mechanisms used to authorise access to your data and services, including accesses to management interfaces
- you are aware of all of the mechanisms by which the service provider would accept management or support requests from you (telephone, web portal, email etc.)
- you can apply granular access control, according to the 'principle of least privilege', enabling both 'standard' and 'administrative' user accounts
- other customers cannot access, modify or otherwise affect your service configuration

You should prefer a cloud provider that:

- makes access control easy to manage at scale, throughout your organisation
- makes it easy to see the access permissions applied to all resources
- uses one access control mechanism for all authorisation decisions
- helps you to remove permissions that are not being used
- lets you apply time-bounded permissions for highly privileged accesses

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-9-secure-user-management

Principle 9: Secure user management - Our comment

Secure user management in Microsoft Azure involves a set of practices and tools designed to effectively manage user identities, access permissions, and roles, ensuring that only authorised individuals can access Azure resources in a secure manner. Here's how secure user management is implemented in Azure:

1. **Azure Active Directory (AAD):**
   - **Identity and Access Management:** AAD is the primary tool for managing user identities in Azure. It provides identity services that support various authentication methods, including multi-factor authentication (MFA) and single sign-on (SSO) across cloud and on-premises environments.
   - **Conditional Access Policies:** These policies provide granular control over how and when users can access Azure resources based on conditions such as location, device state, and risk level.
2. **Role-Based Access Control (RBAC):**
   - **Granular Access Control:** RBAC is used to assign permissions to users, groups, service principals, and managed identities. Permissions are based on roles, with each role defining a set of actions that can be performed.
   - **Least Privilege Principle:** Users are granted only the access they need to perform their tasks, minimising the risk of unauthorised access or actions.
3. **Multi-Factor Authentication (MFA):**
   - **Enhanced Security for Sign-Ins:** MFA requires users to provide two or more verification factors to gain access to Azure resources, significantly reducing the likelihood of unauthorised access.
4. **Privileged Identity Management (PIM):**
   - **Just-in-Time Access:** PIM reduces risks associated with privileged accounts by providing just-in-time privileged access and requiring approval to activate privileged roles.
   - **Access Reviews:** Regular reviews of privileged roles help ensure that only the necessary users have elevated access.
5. **Monitoring and Reporting:**
   - **Audit Logs and Sign-In Reports:** Azure provides detailed logs and reports for auditing and monitoring user access and activities. This includes sign-in logs, audit logs, and reports on user access to resources.
   - **Azure Monitor and Azure Sentinel:** These tools can be used for more advanced monitoring, alerting, and analysis of security-related events.
6. **Governance and Compliance:**
   - **Azure Policy:** This service helps enforce organisational standards and assess compliance with policies, including those related to user access and identity management.
   - **Regulatory Compliance:** Azure ensures compliance with various standards and regulations, providing tools and documentation to assist in managing user access in a compliant manner.
7. **User Education and Awareness:**
   - **Security Awareness Training:** Educating users about security best practices, phishing risks, and safe online behavior is crucial for maintaining a secure Azure environment.
8. **Guest and External User Management:**
   - **Azure B2B Collaboration:** This feature allows secure sharing of Azure services and resources with users from outside the organisation, providing controlled access in line with organisational policies.

Secure user management in Azure is a comprehensive approach that involves not just the technical implementation of identity and access controls, but also governance, compliance, and continuous monitoring. By leveraging these tools and practices, organisations can ensure secure and efficient management of user access to Azure resources.

Principle 10: Identity and authentication

Access to service interfaces should be constrained to authenticated and authorised individuals.

Services and data should only be accessible to an authenticated and authorised identity, which may be either a user or a service identity.

To apply effective access control as described in Principle 9: secure user management, you must have confidence in the authentication method used to determine the identity performing the access.

Weak authentication to these interfaces may enable unauthorised access to your systems, resulting in the theft or modification of your data, changes to your service, or a denial of service. Importantly, authentication should occur over secure channels, as described in Principle 1: data in transit protection.

Goals

You should be sufficiently confident that:

- you understand how access to external interfaces is authenticated
- the cloud provider has a modern password policy and requires multi-factor authentication (MFA) for user accesses
- the cloud provider performs equally robust authentication of service identities as it does for users
- authentication of users will integrate with your processes for managing joiners, movers, and leavers
- processes are available for managing the lifecycle of service credentials

You should prefer a cloud provider that:

- takes active measures to identify and revoke breached credentials
- gives users of the service confidence that they are connecting to the authentic service
- prompts administrators to re-verify themselves using MFA when performing high privilege actions

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-10-identity-and-authentication

Principle 10: Identity and authentication - Our comment

Identity and authentication in Microsoft Azure are fundamental to its security architecture, ensuring that only authorised users can access resources. Azure provides a comprehensive set of tools and services for managing identities, authenticating users, and controlling access to resources. Here's an overview:

1. **Azure Active Directory (AAD):**
   - **Primary Identity Service:** AAD is a cloud-based identity and access management service. It is the backbone for identity management in Azure, providing a secure, scalable, and highly available identity platform.
   - **Single Sign-On (SSO):** AAD enables SSO, allowing users to sign in once and access multiple services and applications without the need to re-authenticate.
   - **Integration with On-Premises Identity Solutions:** AAD can be integrated with on-premises identity solutions, such as Active Directory, through Azure AD Connect.
2. **Multi-Factor Authentication (MFA):**
   - **Enhanced Security:** MFA adds an additional layer of security by requiring users to provide two or more verification methods to access Azure resources, beyond just a password.
   - **Various Verification Methods:** These methods include phone calls, text messages, or notifications through the Microsoft Authenticator app.
3. **Role-Based Access Control (RBAC):**
   - **Fine-Grained Access Control:** RBAC in Azure provides a way to grant users and groups specific permissions to Azure resources. Permissions can be as broad as full administrative access or as narrow as read-only access to specific resources.
   - **Predefined and Custom Roles:** Azure includes many predefined roles and also allows the creation of custom roles to meet specific organisational needs.
4. **Conditional Access:**
   - **Context-Aware Access Policies:** Conditional Access policies in Azure AD enable organisations to define specific conditions under which users can access Azure resources. These policies can consider factors like user location, device health, and risk level.
5. **Azure AD B2B (Business-to-Business):**
   - **External Collaboration:** Azure AD B2B allows organisations to securely share their applications and services with guest users from any other organisation while maintaining control over their own corporate data.
6. **Azure AD B2C (Business-to-Consumer):**
   - **Consumer Identity Management:** Azure AD B2C is a customer identity access management solution, enabling external customers to use their preferred social, enterprise, or local account identities to get single sign-on access to applications and APIs.
7. **Identity Protection:**
   - **Automated Security:** Azure AD Identity Protection leverages machine learning to detect anomalies and suspicious activities that indicate potential identity-based threats. It provides risk-based conditional access to protect Azure resources.
8. **Privileged Identity Management (PIM):**
   - **Just-In-Time Access:** PIM helps manage, control, and monitor access within Azure AD, Azure, and other Microsoft Online Services for users with privileged roles, offering just-in-time privileged access.
9. **Compliance and Regulatory Standards:**
   - **Standards and Certifications:** Azure AD services comply with key international and industry-specific compliance standards, such as ISO 27001, HIPAA, and GDPR.

Identity and authentication in Azure are about ensuring that the right individuals have the right access to the right resources in the right context. By leveraging these tools and services, organisations can enhance their security posture while providing a seamless user experience.

Principle 11: External interface protection

All external or less trusted interfaces to the service should be identified and defended.

Defensive measures may include application programming interfaces (APIs), web consoles, command line interfaces (CLIs), or direct connect services. Also, the cloud provider's administration interfaces, the interfaces you use to access the service, and any interfaces to your services built on top of the cloud service.

If some of the interfaces exposed are private (such as management interfaces) then the impact of compromise may be more significant. You can use different models to connect to cloud services which expose your enterprise systems to varying levels of risk.

Goals

You should be sufficiently confident that:

- you understand what physical and logical interfaces to your information exist, and how access to your data is controlled
- the service identifies and authenticates users to an appropriate level over those interfaces (as described in Principle 10)

You should prefer a cloud provider that:

- shows you which interfaces or services are exposed to the internet, highlighting those exposed without authentication
- makes it easy to understand which defences are in place to protect each external interface to your data or your use of the service
- provides easy to use defences against common attacks for the interfaces and components you use to build your service

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-11-external-interface-protection

Principle 11: External interface protection - Our comment

External interface protection in Microsoft Azure refers to the security measures implemented to protect the interfaces through which Azure services are accessed and interacted with from outside the Azure network. This includes protection against unauthorised access, data breaches, and various cyber threats. Effective external interface protection is crucial for safeguarding data and maintaining the integrity and availability of services. Here's how Azure addresses this:

1. **Azure Firewall:**
   - **Centralised Network Security:** Azure Firewall is a managed, cloud-based network security service that protects Azure Virtual Network resources. It provides a barrier between Azure resources and the outside world.
   - **Intelligent Filtering:** It offers features like application-level filtering, network-level filtering, and threat intelligence-based filtering.
2. **Web Application Firewall (WAF):**
   - **Protection for Web Apps:** Azure's WAF, available with Azure Application Gateway, provides centralised protection of web applications from common exploits and vulnerabilities.
   - **Customisable Rules:** WAF allows customisation of rules to meet specific application requirements and to protect against attacks such as SQL injection and cross-site scripting (XSS).
3. **Azure DDoS Protection:**
   - **Mitigation of DDoS Attacks:** This service provides protection to Azure-hosted applications from distributed denial-of-service (DDoS) attacks, ensuring the availability and performance of applications even under attack.
   - **Adaptive Tuning:** Azure DDoS Protection uses adaptive tuning based on network traffic patterns to detect and mitigate threats.
4. **Network Security Groups (NSGs) and Virtual Networks:**
   - **Traffic Filtering:** NSGs are used to filter network traffic to and from Azure resources in an Azure Virtual Network. They can be used to define security rules that allow or deny traffic based on direction, protocol, source address and port, and destination address and port.
   - **Network Isolation and Segmentation:** Virtual Networks provide isolation and segmentation, allowing for the creation of private networks within Azure.
5. **Azure Virtual WAN:**
   - **Unified Network Infrastructure:** This service provides a unified wide area network, integrating networking, security, and routing functionalities to provide high availability and reliable connectivity.
6. **TLS/SSL Encryption:**
   - **Encryption in Transit:** Azure ensures that data transmitted to and from Azure services is protected using TLS/SSL encryption, safeguarding data against interception and tampering.
7. **API Management:**
   - **Secure API Gateway:** Azure API Management allows organisations to publish, manage, secure, and analyze APIs in a secure and scalable environment. It includes features like rate limiting, IP filtering, and CORS management.
8. **Identity and Access Management:**
   - **Azure Active Directory (AAD):** AAD and its integration with services provide secure identity management and access control. Features like multi-factor authentication and conditional access policies add layers of security.
9. **Monitoring and Detection:**
   - **Azure Sentinel and Azure Security Centre:** These tools provide advanced threat detection, security analytics, and proactive monitoring to identify and mitigate threats.
10. **Compliance and Standards:**
    - **Regulatory Adherence:** Azure complies with various international and industry-specific standards, ensuring that the external interfaces are secured according to global best practices.

By implementing these comprehensive security measures, Azure ensures that external interfaces to its services are robustly protected, minimising the risk of unauthorised access and cyber threats.

Principle 12: Secure service administration

Cloud providers should recognise the high value of administration systems.

The design, implementation, and management of the cloud provider's administration systems used by your cloud provider should follow enterprise good practice, whilst recognising their high value to attackers.

Systems used by the vendor for administration of their cloud services will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

Goals

You should be sufficiently confident that your provider:

- builds and maintains trust in the devices it uses to administer the service, with regular and thorough, security assessments
- protects its administration interfaces
- risk-manages its administration using tiers
- uses privilege access management, including 'just in time' and 'just enough' administration
- uses administration interfaces that produce detailed audit information, which is checked regularly for anomalous or unexpected behaviour

You should prefer a cloud provider that:

- uses layered controls and processes to manage service administration, avoiding the browse-up anti-pattern

These concepts are covered in more detail in the NCSC's Secure system administration guidance.

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-12-secure-service-administration

Principle 12: Secure service administration - Our comment

Secure service administration in Microsoft Azure involves a set of practices and technologies designed to ensure that the management of Azure services is conducted in a secure and controlled manner. This includes protecting the administration of Azure resources from unauthorised access and actions, and ensuring that administrative tasks are performed with minimum risk. Here's an overview of how secure service administration is implemented in Azure:

1. **Role-Based Access Control (RBAC):**
   - **Granular Access Control:** RBAC is used to provide fine-grained access control to Azure resources. Administrators can assign roles to users, groups, and service principals, defining what actions they can perform.
   - **Least Privilege Principle:** Following this principle, administrators grant users only the access that they need to perform their jobs, minimising the potential for unauthorised or accidental changes.
2. **Azure Active Directory (AAD):**
   - **Identity Management:** AAD is the primary tool for managing identities in Azure. It supports multi-factor authentication (MFA) and conditional access policies to enhance the security of administrative access.
   - **Integration with Services:** AAD integrates with various Azure services to manage identities and access to resources securely.
3. **Privileged Identity Management (PIM):**
   - **Just-in-Time Access:** PIM reduces the risks associated with privileged accounts by providing time-bound and approval-based role activation, ensuring that elevated access is granted only when needed.
   - **Access Reviews:** Regular reviews of access rights help ensure that only necessary personnel have elevated access.
4. **Azure Policy:**
   - **Policy Enforcement:** Azure Policy helps enforce organisational standards and assess compliance at scale, allowing administrators to create and assign policies that enforce rules over Azure resources.
5. **Monitoring and Logging:**
   - **Azure Monitor and Azure Activity Log:** These services provide data and insights to monitor the health and performance of Azure resources and track administrative operations.
   - **Azure Sentinel:** Offers advanced threat detection, security analytics, and proactive monitoring of security-related events.
6. **Network Security Controls:**
   - **Network Security Groups (NSGs) and Azure Firewall:** These tools provide network-level filtering to control inbound and outbound traffic to Azure resources, helping secure administrative access.
   - **Virtual Network (VNet) and Subnet Design:** Proper design of VNets and subnets ensures secure segmentation and control of traffic flow.
7. **Secure Access to Management Interfaces:**
   - **VPN and ExpressRoute:** These services provide secure and private connectivity to Azure for managing resources.
   - **Azure Bastion:** Offers secure and seamless RDP/SSH connectivity to virtual machines directly from the Azure portal over SSL.
8. **Automation for Compliance and Remediation:**
   - **Azure Automation:** This service helps automate repeated tasks and processes, ensuring that resources remain in compliance with desired configurations.
9. **Encryption and Key Management:**
   - **Azure Key Vault:** Used to manage cryptographic keys and other secrets used in cloud applications and services, enhancing the security of administrative tasks.
10. **Compliance and Regulatory Standards:**
    - Azure ensures compliance with various international and industry-specific standards, providing a secure and compliant environment for service administration.

Secure service administration in Azure is about ensuring that the management of cloud resources is conducted in a controlled, secure, and compliant manner, reducing risks and protecting against potential security threats.

Principle 13: Audit information and alerting for customers

Providers should supply logs needed to monitor access to your service, and the data held within it.

You should be able to identify security incidents and should have the information necessary to determine how and when they occurred.

This will require:

- audit information
- security alerts

Principle 13.1: audit information

Goals

You should be provided with the audit data needed to investigate incidents related to your use of the service and the data held within it. The type of audit information available to you will have a direct impact on your ability to respond to inappropriate or malicious activity within reasonable timescales.

You should be sufficiently confident that:

- you are aware of the audit information that will be provided to you, how and when it will be made available, the format of the data, and the retention period associated with it
- the audit information available will meet your needs for investigating misuse or incidents
- the provider will supply relevant audit information for actions taken by its personnel that affect your service (or the data held within it)
- audit information cannot be deleted by the customer or the cloud provider during a defined retention period

You should prefer a cloud provider that:

- either enables all audit information services by default, or makes them easy to enable
- provides APIs and tooling to query, process, and archive audit information
- implements an RBAC role for auditors to review logs without needing wider privileges

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-13-audit-information-and-alerting-for-customers

Principle 13.1: audit information - Our comment

Audit information in Microsoft Azure is an essential component of cloud security and compliance. It involves the collection, retention, and analysis of logs and data that provide insight into the operations, usage, and performance of Azure resources, as well as the actions taken by users and administrators within the Azure environment. Effective auditing helps in detecting and investigating security incidents, ensuring compliance with regulations, and optimising resource performance. Here's an overview of how audit information is handled in Azure:

1. **Azure Activity Log:**
   - **Operational Insights:** The Azure Activity Log provides insight into subscription-level events, including management operations performed in Azure Resource Manager. This log includes a range of data such as who performed the operation, when it was performed, and the status of the operation.
   - **Integrated with Azure Monitor:** The Activity Log can be integrated with Azure Monitor for more comprehensive monitoring and analysis.
2. **Azure Monitor Logs:**
   - **Comprehensive Data Collection:** Azure Monitor collects and aggregates data from a variety of sources, including application telemetry, cloud resources, and user and administrator activities.
   - **Log Analytics:** This feature allows you to query and analyze the collected data, helping you understand the performance and operation of your Azure and non-Azure resources.
3. **Azure Security Centre:**
   - **Security Auditing and Reporting:** Azure Security Centre provides advanced threat detection, security health monitoring, and compliance reporting. It helps in identifying and addressing potential security issues in your Azure resources.
4. **Azure Audit Logs for Services:**
   - **Service-Specific Logs:** Many Azure services, like Azure SQL Database, Azure Virtual Machines, and Azure Storage, provide their own audit logs, which track service-specific operations and events.
5. **Azure AD Audit Logs and Sign-in Logs:**
   - **User and Administrator Activity:** Azure AD provides audit logs that include records of system activities like adding or removing users, changing user roles, and updating applications. Sign-in logs track user authentication and authorisation activities.
6. **Compliance and Regulatory Requirements:**
   - **Data Retention Policies:** Azure allows you to set data retention policies to meet compliance requirements, ensuring that audit logs are retained for the required period.
   - **Export Capabilities:** Audit data can be exported to external systems for further analysis or for compliance reporting purposes.
7. **Integration with Third-Party Tools:**
   - **SIEM Integration:** Azure supports integration with third-party Security Information and Event Management (SIEM) systems, like Splunk or Azure Sentinel, for enhanced analysis and correlation of audit data.
8. **Azure Policy Compliance Data:**
   - **Policy Enforcement and Compliance Reporting:** Azure Policy provides detailed compliance data, helping you ensure that your resources conform to your company's internal policies and external regulatory requirements.
9. **Access and Use Controls:**
   - **Role-Based Access Control (RBAC):** RBAC can be used to control access to audit information, ensuring that only authorised personnel can view or modify this data.
10. **Alerting and Notification:**
    - **Proactive Monitoring:** You can set up alerts based on specific metrics or log queries to get notified of potential issues identified in the audit logs.

By effectively managing and analyzing audit information, organisations can enhance their security posture, ensure regulatory compliance, and gain valuable insights into their Azure environment's operational health and performance.

Principle 13.2: security alerts

Goals

You should be provided with alerts when the cloud provider detects attacks against your data, or your use of their services. The cloud provider should be your first line of defence for identifying and preventing common attacks.

You should be sufficiently confident that:

- the provider will alert you when they identify attacks against, or vulnerabilities in, your use of their services
- the provider will alert you when they detect attempted or successful compromise of your data held in their services
- the provider will send their alerts promptly to a recipient of your choosing, through an automated means

You should prefer a cloud provider that:

- will alert you when your configuration of their services results in security issues
- will make it easy to receive and respond to alerts automatically

Principle 13.2: security alerts - Our comment

Security alerts in Microsoft Azure are notifications generated by Azure services when they detect potential security threats or suspicious activities within an Azure environment. These alerts play a crucial role in the early detection and response to security incidents, helping to maintain the integrity and security of Azure resources. Here's an overview of how security alerts are managed in Azure:

1. **Azure Security Centre:**
   - **Threat Detection and Alerts:** Azure Security Centre automatically collects, analyzes, and integrates log data from various Azure resources. It uses advanced analytics and global threat intelligence to detect and generate alerts on potential threats, such as unusual network traffic, potential malware installation, or attempts to access sensitive resources.
   - **Prioritised Alerting:** Alerts are prioritised based on severity, helping administrators focus on the most critical threats first.
2. **Azure Sentinel:**
   - **SIEM and SOAR:** Azure Sentinel is a scalable, cloud-native SIEM (Security Information and Event Management) and SOAR (Security Orchestration Automated Response) solution. It provides advanced threat detection, threat visibility, proactive hunting, and threat response.
   - **Alerts and Incidents:** Sentinel aggregates data from various sources, including Azure services, on-premises equipment, and other cloud providers, to generate security alerts. It also allows you to create custom detection rules.
3. **Azure Monitor:**
   - **Integrated Monitoring:** Azure Monitor provides comprehensive monitoring of Azure resources, including the generation of security alerts based on the monitoring data.
   - **Alert Rules:** Administrators can create custom alert rules in Azure Monitor based on metrics or logs to detect abnormal activity or conditions.
4. **Email Notifications:**
   - **Automated Notifications:** When an alert is triggered, Azure can automatically send email notifications to the designated recipients, such as IT administrators or security personnel.
5. **Integration with Third-Party Tools:**
   - **SIEM Integration:** Security alerts from Azure can be integrated with third-party SIEM systems for further analysis and correlation.
   - **API Access:** Azure provides APIs for retrieving alert information, which can be used to integrate with custom applications or other security tools.
6. **Actionable Insights and Recommendations:**
   - **Guidance and Remediation Steps:** Azure Security Centre and Azure Sentinel provide actionable insights and recommendations for investigating alerts and remediating threats.
7. **Customisation and Configuration:**
   - **Custom Alert Rules:** Organisations can create custom alert rules tailored to their specific environment and security needs.
   - **Alert Suppression Rules:** To reduce noise, administrators can configure rules to suppress alerts that are known to be benign.
8. **Compliance and Regulatory Considerations:**
   - **Audit Trails and Compliance Reporting:** Security alerts and the corresponding responses can be logged for audit trails and compliance reporting.

Security alerts in Azure enable organisations to quickly detect and respond to potential security issues, helping to minimise the risk to their cloud environment. By leveraging Azure's security alert capabilities, organisations can maintain a robust security posture in their cloud operations.

Principle 14: Secure use of the service

Providers should make it easy for you to adequately protect your data.

Your cloud provider should make it easy for you to meet your responsibility to adequately protect your data.

You should consider:

- whether the service is secure by design and by default
- what help the provider gives you to meet your responsibilities

Principle 14.1: Security by design and by default

Goals

Your service provider should make it easy for you to use their services in a way that is defended against common attacks.

You should be sufficiently confident that:

- you know which goals from the Principles 1-13 are met by the service's default configuration
- you know what you need to do to the service's configuration to meet the remaining goals
- data and services are not accessible to unauthenticated users, by default
- the provider takes responsibility for improving their service's default configuration, to respond to new threats (this may include altering the configuration of existing customers, as well as changing the starting point for new customers)

You should prefer a cloud service that:

- meets all of the goals described in Principles 1-13 by design, or in its default configuration
- makes configurable security-enhancing features opt-out, and not opt-in
- defends against common network-based attacks (such as DDoS) against the service and your hosted workloads by default, as described in Principle 11: external interface protection

For suggested implementation approaches, see National Cyber Security Centre page reference:

https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-14-secure-use-of-the-service

Principle 14.1: Security by design and by default - Our comment

"Security by design" and "security by default" are fundamental principles that guide the architecture and operation of Microsoft Azure. These principles ensure that security is integrated into the fabric of Azure's services and infrastructure from the outset and that the default configurations of services are set to secure settings. Here's how these principles are applied in Azure:

1. **Security by Design:**
   - **Secure Development Lifecycle (SDL):** Azure services are developed using Microsoft's SDL, which integrates security and privacy in all phases of development. This includes risk assessments, security design reviews, threat modeling, code analysis, and penetration testing.
   - **Built-in Security Features:** Azure incorporates built-in security features like network security, identity management, encryption, and access controls into its services.
   - **Regular Security Updates and Patches:** Azure continually updates its infrastructure and services with the latest security patches and updates.
2. **Security by Default:**
   - **Default Secure Settings:** Azure services are configured with secure defaults. This means that when a service is deployed, its default configuration settings are set to secure options, reducing the risk of misconfiguration.
   - **Minimal Exposure:** Services are designed to minimise exposure to threats. For example, Azure Storage accounts are created with secure defaults such as denying public access.
   - **Role-Based Access Control (RBAC):** Azure implements RBAC with least privilege access as a default, ensuring that users and services have only the permissions necessary to perform their intended functions.
3. **Data Protection:**
   - **Encryption at Rest and in Transit:** Azure provides encryption for data at rest and in transit by default, protecting data from unauthorised access.
   - **Backup and Disaster Recovery:** Azure's built-in features for backup and disaster recovery ensure that data integrity and availability are maintained.
4. **Network Security:**
   - **Secure Network Architecture:** Azure's default network architecture is designed for security, including features like DDoS protection, NSGs (Network Security Groups), and Azure Firewall.
   - **Private Connectivity Options:** Services like Azure Virtual Network and ExpressRoute offer secure, private connectivity options.
5. **Compliance and Certifications:**
   - **Regulatory Compliance:** Azure meets a broad set of international and industry-specific compliance standards, ensuring that its services are designed in accordance with stringent security requirements.
6. **Monitoring and Threat Detection:**
   - **Azure Security Centre:** This provides unified security management and advanced threat protection, enabling visibility and control over the security of Azure resources.
   - **Continuous Monitoring and Analytics:** Azure automatically monitors for security threats and provides analytics to detect anomalous activities.
7. **Identity and Access Management:**
   - **Azure Active Directory (AAD):** AAD offers robust identity services with features like multi-factor authentication and conditional access, enhancing the security of user access.
8. **Educational Resources and Best Practices:**
   - **Guidance and Tools:** Azure provides extensive documentation, tools, and best practices to help users understand and implement security effectively in their cloud environments.

By integrating these security principles into its cloud environment, Azure ensures that its infrastructure and services are resilient to threats and vulnerabilities, providing a secure foundation for its users' applications and data.

Principle 14.2: Help customers meet their security responsibilities

Goals

Your service provider should make it easy for you to be confident that you are using the cloud securely. It should be easy for you to see what services you have in the cloud, and how they have been configured.

You should be confident that:

- all service configuration can be set and audited using infrastructure as code, or via an API
- there is a single place where you can see all of your deployed resources across all services and regions offered by that cloud platform
- all service configurations are visible and intuitive to humans, so that they can easily audit what services they are using, where their data is, and how those services are configured

You should prefer a provider that:

- raises an actionable alert when your configuration of the service could weaken your security stance, or leave you vulnerable to a breach
- gives you tools to help meet your responsibilities, such as hardened container base images, CI/CD tooling, and detection of common vulnerabilities in the applications that you deploy
- monitors the workloads you deploy for out-of-date dependencies and missing security updates. The service may raise a security alert or automatically remediate the problem

Principle 14.2: Help customers meet their security responsibilities - Our comment

In the Microsoft Azure cloud environment, security is a shared responsibility between Microsoft and its customers. While Microsoft ensures the security of the cloud infrastructure, customers are responsible for securing their operations within the cloud. To help customers meet their security responsibilities, Azure provides a range of tools, services, and guidance. Here's how Azure supports customers in maintaining a secure cloud environment:

1. **Security and Compliance Documentation:**
   - **Guidance and Best Practices:** Azure offers extensive documentation covering security best practices, architecture guidelines, and compliance information. This includes the Azure Security Centre, Azure compliance documentation, and the Azure Architecture Centre.
   - **Security Benchmarks:** Azure provides security benchmarks and checklists that help customers understand and implement security controls effectively.
2. **Identity and Access Management:**
   - **Azure Active Directory (AAD):** AAD offers robust identity services, including multi-factor authentication (MFA) and conditional access, which customers can use to secure user access to their Azure resources.
   - **Role-Based Access Control (RBAC):** Azure implements RBAC to provide fine-grained access control to Azure resources.
3. **Network Security:**
   - **Network Security Groups (NSGs) and Azure Firewall:** These tools enable customers to create secure network environments with controlled access to and from Azure resources.
   - **Virtual Private Networks (VPNs) and ExpressRoute:** Azure offers VPN and ExpressRoute for establishing secure connections to Azure.
4. **Data Protection:**
   - **Encryption:** Azure provides encryption capabilities for data at rest and in transit, such as Azure Storage Service Encryption and Azure SQL Database Transparent Data Encryption (TDE).
   - **Azure Key Vault:** This service allows customers to manage cryptographic keys and other secrets used by cloud applications and services.
5. **Security Monitoring and Threat Detection:**
   - **Azure Security Centre:** Offers advanced threat protection, security health monitoring, and compliance reporting.
   - **Azure Sentinel:** A cloud-native SIEM solution that provides intelligent security analytics across the enterprise.
6. **Compliance Support:**
   - **Compliance Offerings:** Azure aligns with various international and industry-specific compliance standards, providing tools and documentation to assist customers in meeting regulatory requirements.
   - **Azure Policy:** Helps enforce organisational standards and assess compliance at scale.
7. **Incident Response and Recovery:**
   - **Azure Site Recovery and Azure Backup:** These services provide disaster recovery and data backup capabilities to ensure business continuity.
   - **Guidance on Incident Response:** Azure offers guidance and best practices for responding to security incidents.
8. **Application Security:**
   - **Web Application Firewall (WAF):** Available with Azure Application Gateway to protect web apps from common vulnerabilities.
   - **Secure DevOps Kit for Azure (AzSK):** Includes tools and practices for securely developing applications in Azure.
9. **Customer Education and Awareness:**
   - **Azure Security Blog and Webinars:** Microsoft provides regular updates, security tips, and educational content through its blog and webinars.
   - **Azure Training and Certifications:** Azure offers various training programs and certifications focusing on security and compliance.
10. **Consultative Support:**
    - **Azure Support Plans:** Microsoft offers different levels of support plans, including options where customers can get direct help from Azure security experts.

By leveraging these tools, services, and guidance, Azure customers can effectively manage their security responsibilities in the cloud, protecting their applications, data, and infrastructure from potential threats.