Microsoft Azure Well-Architected Framework - Security Pillar

www.thecyphere.com info@thecyphere.com

Learn and adopt Microsoft Azure security pillars to ensure stable, efficient and secure systems while focusing on functional requirements.

www.thecyphere.com **info@thecyphere.com**

01. Security design principles

www.thecyphere.com info@thecyphere.com

Ensures a strong system, whether on the cloud, on-premises, or hybrid.

They enhance security for confidentiality, integrity, and availability, covering the following:

- Resource planning and hardening.
- Automation with least privilege.
- Data classification and encryption.
- System security monitoring and incident response planning.

- Endpoint identification and protection.
- Defence against code-level vulnerabilities.
- Modelling and testing for potential threats.

02. Governance, risk, and compliance

Governance

It involves overseeing, auditing, reporting, ensuring effectiveness, monitoring improvements, adapting to new requirements, and meeting reporting obligations.

Risk

Refers to potential harm to an organisation's information, systems, and operations, including security issues and their potential impact.

Compliance

Practice of adhering to specific laws, regulations, standards, and guidelines established by government bodies, and industry associations.

03. Regulatory compliance

www.thecyphere.com info@thecyphere.com

Mandate organisations to adhere to security standards for due diligence, affecting architecture, PaaS/SaaS choices, configuration, and workload operations.

04. Adminstration

Involves overseeing and operating IT systems to meet business service levels that could pose high-security risks due to privileged access.

Best practices

- Minimise the number of critical impact admins.
- Managed accounts for admins.
- No standing access / just-in-time privileges.

- Apply admin workstation security.
- Passwordless or multifactor authentication for admins.
- Attack simulation for critical impact accounts.
- Use built-in roles.

- Enforce conditional access for admins - Zero Trust.
- Avoid granular and custom permissions.
- Establish lifecycle management for critical impact accounts.

05. Applications and services

www.thecyphere.com info@thecyphere.com

Cloud platform applications store

business value but carry risks through data handling and processes.

www.thecyphere.com **info@thecyphere.com**

Identifying systems with significant access is vital, as they can potentially control other critical systems or data.

06. Identity and access management

Design and operate workloads sustainably, emphasising energy efficiency, resource utilisation, and alignment with environmental goals.

Best practices

- Define clear roles and access limits.
- Use Azure RBAC with built-in roles.
- Apply management locks for resource protection.
- Implement managed identities.

- Sync enterprise directories.
- Employ Azure AD Conditional Access.
- Separate identities for non-employees.
- Prioritise passwordless.
- Block legacy authentication methods.

Azure services for identity

- Azure AD
- Azure AD B2B
- Azure AD B2C

07. Information protection and storage

Involve safeguarding and managing data within the Azure cloud environment.

This includes ensuring data confidentiality, integrity, availability, and compliance.

Best practices

- Use Identity-based storage access controls.
- Encrypt virtual disk files.
- Enable platform encryption services.
- Encrypt data in transit.

08. Network security and containment

www.thecyphere.com info@thecyphere.com

Involves implementing measures to protect and isolate your Azure resources to ensure they are shielded from unauthorised access and threats.

Best practices

- Segment and secure network communication.
- Implement traffic and access controls.
- Protect public endpoints with Azure services.
- Guard against DDoS attacks.

- Ensure VM security with NAT Gateway.
- Control internal and external network traffic.
- Employ defence-in-depth for data protection.

Azure Services for network security

- Azure Virtual Network
- Azure Firewall
- Azure NAT Gateway
- Azure ExpressRoute
- Azure Private Link
- Azure DDoS Protection

09. Security operations

www.thecyphere.com info@thecyphere.com

Essential for preserving and restoring Azure system security.

It encompasses monitoring, detecting, responding to, and mitigating security threats and incidents.

Best practices

- Prioritise alert and log integration.
- Ensure hybrid estate visibility through tools and skills.
- Favour built-in cloud security controls.

- Rapidly remediate adversaries.
- Swiftly acknowledge alerts.
- Invest in high-value systems.
- Embrace proactive threat hunting.

www.thecyphere.com **info@thecyphere.com**

Liked this?

Share this post ♻️

Schedule a conversation today:

info@thecyphere.com