AZ-305 Cheat Sheet

High-yield design choices for identity, storage, continuity, and infrastructure on Azure.

BEST FOR	FOCUS	USE WITH
final review	architecture decisions	AZ-104 + practice questions

1. Identity, governance, monitoring

Entra ID + RBAC	Use tenant-level identity plus least-privilege role assignments to control who can access subscriptions, resource groups, and resources.
Policy vs Locks	Use Azure Policy to enforce or audit rules. Use resource locks to prevent accidental delete or modification of critical assets.
Management Groups	Use when you need policy and governance inheritance above the subscription level across multiple landing zones.
Monitor + Log Analytics	Use Azure Monitor for metrics, alerts, and logs; use Log Analytics when you need KQL-based investigation across resources.

2. Storage and data decisions

Blob tiers	Hot for frequent access, Cool for less frequent access, Archive for long-term retention when retrieval delay is acceptable.
Azure Files	Choose for SMB/NFS shared file workloads and lift-and-shift file shares that need managed availability.
Managed disks	Pick disk SKU by workload pattern: Premium SSD for production IO, Standard SSD for balanced cost/performance, Ultra when latency matters.
Data stores	Use Azure SQL for relational PaaS, Cosmos DB for globally distributed low-latency apps, and Storage/ADLS for analytics-scale object data.

3. Business continuity

Availability Zones	Use to protect against datacenter-level failure within a region for zonal or zone-redundant architectures.
Region pairs	Use for broader resilience, update sequencing benefits, and disaster recovery design between paired regions.
Backup vs Site Recovery	Backup protects data and point-in-time restore; Site Recovery orchestrates failover and replication for workloads.
RTO vs RPO	Pick services and topology by tolerated downtime and tolerated data loss rather than by feature popularity.

4. Infrastructure and network

VNet design	Plan address space early, avoid overlap, and separate tiers with subnets, NSGs, and route design.
Connectivity choice	Use VPN Gateway for quick or lower-throughput hybrid links; use ExpressRoute for private, predictable enterprise connectivity.
Load balancing	Use Load Balancer for L4 traffic, Application Gateway for L7 plus WAF, and Front Door for global edge routing.
Compute patterns	Use VM Scale Sets for IaaS scaling, AKS for Kubernetes, and App Service when you want managed web app hosting.

5. Architecture choices

PaaS first	Default to managed services when they satisfy requirements for speed, operations, patching, and built-in resiliency.
Security boundaries	Design with private endpoints, managed identities, Key Vault, NSGs, and least privilege before adding complexity elsewhere.
Cost + operations	Favor services with autoscaling, native backup, and centralized monitoring to reduce long-term operational drag.
Migration fit	Choose refactor, replatform, or rehost based on timeline, skill depth, compliance constraints, and expected business value.