Microsoft AZ-400 Cheat Sheet

One-page cram sheet for DevOps processes, source control, pipelines, security, and instrumentation strategy.

Best for	Focus	Use with
Last review before drills or exam day	High-yield DevOps decisions and pipeline thinking	Use with the quick summary for rapid refresh

1. Processes and communications

Flow of work	Know boards, backlog flow, traceability, and how work moves from idea to deployment.
Metrics	Cycle time, lead time, deployment frequency, and failure rate matter more than vanity metrics.
Collaboration	Good DevOps communication connects dev, ops, security, and product, not just tooling.
Feedback loops	Shorter feedback usually means faster correction and safer delivery.

2. Source control strategy

Branch strategy	Choose simple branching that fits release cadence and team size.
Pull requests	Use reviewers, branch policies, and validation checks to reduce risky merges.
Enterprise Git	Think repo structure, permissions, technical debt, and inner-source style collaboration.
Artifact traceability	Be able to connect commits, builds, packages, releases, and work items.

3. Build and release pipelines

CI fundamentals	Automate build, test, quality checks, and packaging on every meaningful change.
CD patterns	Blue-green, canary, rolling, and ring deployments are exam favorites.
IaC	ARM/Bicep/Terraform-style thinking matters because infra should be repeatable and reviewable.
Pipeline maintenance	A working pipeline today still needs secrets, dependencies, and test strategy kept healthy.

4. Security and compliance

Shift left	Security belongs in source control, pipelines, packages, and policy checks early.
Secrets management	Use managed secret stores; avoid hardcoded credentials and loose variable handling.
Policy and approvals	The best answer often balances speed with required control and auditability.

Supply chain awareness	Packages, dependencies, and signing/trust are part of DevOps security now.

5. Instrumentation strategy

Monitoring	App, infra, logs, traces, and alerts should support quick diagnosis.
Observability	Logs alone are not enough; correlate telemetry and user impact.
Actionable alerts	Alert on symptoms that need action, not every event.
Continuous improvement	Use production insights to tune backlog, architecture, and release process.