CompTIA CASP+ (CAS-004) Cheat Sheet

One-page cram sheet for security architecture, risk, operations, resilience, and reporting. Legacy CAS-004 set.

Best for	Focus	Use with
Last review for legacy notes or comparisons	Architecture decisions + risk tradeoffs + resilience logic	Use with ports sheet and commands sheet

1. Security architecture

Enterprise view	Think architecture across cloud, on-prem, hybrid, identity, network, and data rather than isolated controls.
Defense in depth	The best design layers preventive, detective, and responsive controls instead of trusting one product.
Zero Trust mindset	Verify explicitly, minimize implicit trust, and segment based on identity, device, and workload context.
Tradeoff thinking	CASP-level questions often ask for the best balance of security, resilience, and business practicality.

2. Governance, risk, and compliance

Risk treatment	Avoid, transfer, mitigate, or accept based on business context, not just technical severity.
Policies vs standards	Policies define direction; standards define required specifics; procedures explain how.
Framework alignment	Map controls to business, regulatory, and audit requirements rather than deploying them blindly.
Third-party risk	Vendors, supply chain, and shared-responsibility boundaries are part of enterprise risk.

3. Security engineering and operations

Secure integration	Identity, PKI, logging, SIEM, EDR, DLP, and segmentation work best when integrated.
Monitoring strategy	Logs, telemetry, flows, and endpoint signals must support detection and incident response goals.
High availability	Security controls should not become single points of failure.
Cryptography use	Know when to use encryption, hashing, signing, key exchange, and certificate lifecycle controls.

4. Incident response and resilience

Preparation	Plans, playbooks, backups, and tested recovery paths matter before incidents happen.

Containment vs recovery	Stop spread first, restore safely second, then fix root cause.
Forensics awareness	Evidence handling, timestamps, and chain of custody still matter at architect level.
Lessons learned	Mature programs feed incident findings back into architecture and control design.

5. Collaboration and reporting

Audience fit	Executives want risk and resilience; engineers need technical detail and implementation actions.
Business language	Translate security choices into impact, cost, risk reduction, and operational sustainability.
Strategic prioritization	Not every issue deserves the same urgency; align work with crown-jewel assets and exposure.
Architect mindset	Choose solutions that scale across teams, environments, and future change.