Cloud Security Professional (CCSP) — One-Page Study Guide

A) Exam Snapshot

Target role level: Intermediate to advanced

- **Issuer:** ISC2
- **Exam code:** CCSP
- **Format:** Computerized Adaptive Testing (CAT) - effective Oct 1, 2025
- **Time / items:** 3 hours; 100-150 items (adaptive)
- **Question types:** multiple-choice + advanced item types
- **Passing:** 700 / 1000 (scaled) | **Notes:** [VERIFY: CAT review/backtracking rules]

B) Domain Weights

Domain	Weight
Cloud Concepts, Architecture and Design	17%
Cloud Data Security	20%
Cloud Platform & Infrastructure Security	17%
Cloud Application Security	17%
Cloud Security Operations	16%
Legal, Risk and Compliance	13%

C) Core Workflow (How the exam thinks)

- Confirm service model and shared responsibility boundary before choosing controls.
- Classify the data and map its lifecycle (create, store, use, share, archive, destroy).
- Select controls at the right layer: identity, network, compute, storage, and application.
- Prefer answers that are provable: configs, logs, tickets, approvals, and third-party reports.
- Check detection and response realism: monitoring coverage, alert quality, and evidence handling.
- Finish with governance: policy, risk acceptance, compliance mapping, and vendor oversight.

D) High-Yield Concepts

- Shared responsibility by **IaaS / PaaS / SaaS** (ownership of controls and evidence).
- Cloud deployment models and trust boundaries (public, private, hybrid, community).
- Data residency, privacy, and cross-border transfer constraints (PII and regulated data).
- Encryption at rest vs in transit, plus key ownership and auditability (KMS, HSM, BYOK).
- Identity and access management (IAM): least privilege, federation, MFA, privileged access.
- Network patterns: segmentation, security groups, micro-segmentation, and zero trust concepts.
- Virtualization and container risk: multi-tenancy, image provenance, and isolation failures.
- Secure SDLC in cloud: threat modeling, CI/CD controls, secrets management, API security.
- Logging and monitoring: integrity, centralization, and decision-quality alerts.
- BC/DR fundamentals: recovery time objective (RTO) vs recovery point objective (RPO).

E) Common Traps

- Assuming the provider handles all security or compliance duties (shared responsibility).
- Skipping the first step: identifying the service model and what layers are visible to the customer.
- Treating encryption as a full answer while ignoring key access, rotation, and logging.
- Missing identity paths: excessive roles, unmanaged service accounts, or weak federation rules.
- Confusing backups with recovery readiness; forgetting restore testing and dependency mapping.
- Using weak proof: screenshots without timestamps, logs without clock source, missing approvals.

F) Cheat Sheet (Artifacts & shorthand)

- **IaaS**: customer secures OS and above. **PaaS**: customer secures app and data. **SaaS**: customer secures identity and configuration.
- Data states: **in transit**, **at rest**, **in use**; match controls and evidence to each state.
- Key questions: who owns the keys, who can decrypt, and where admin actions are logged.
- Assurance artifacts: SOC reports, ISO 27001 certificates, audit letters, CSA STAR entries.
- Operational evidence: IAM role listings, security group rules, flow logs, change tickets, approvals.
- Risk actions: avoid, mitigate, transfer, accept; record rationale and approver identity.
- Contract clauses to recognize: breach notice timing, right to audit, subcontractor flow-down, data ownership.

G) Exam-Day Tactics

- Read for the decision: control choice, evidence adequacy, or risk judgment (not trivia).
- Eliminate answers that violate the stated constraints (jurisdiction, classification, service model).
- Prefer verifiable answers: control plus proof trail (who acted, what changed, where recorded, when).
- If two options look right, choose the one that reduces root risk first (identity and data are common roots).
- Keep pace steady for CAT; avoid long stalls and commit to the best-supported choice.
- [VERIFY: CCSP CAT rules for reviewing or changing prior items at Pearson VUE]

H) 30-Minute Final Review Plan

- Recall one anchor per domain and one common evidence artifact that proves it.
- Rehearse shared responsibility for IaaS/PaaS/SaaS and typical ownership pitfalls.
- Run a data lifecycle pass: classification, residency, encryption, key ownership, retention, disposal.
- Run an IAM pass: least privilege, federation, MFA, admin logging, and privileged access.
- Run an assurance pass: which reports prove what, and what gaps require contract or testing evidence.
- Do five micro-scenarios: model, top risk, best control, and best evidence in one sentence.