Certified Chief Information Security Officer (CCISO) — One-Page Study Guide

A) Exam Snapshot

Exam: Certified Chief Information Security Officer (CCISO) — Issuer: EC-Council

Format: 150 multiple-choice questions; cognitive levels: knowledge, application, analysis.

Time limit: 2.5 hours (150 minutes). Passing score: cut score varies by form (60%–85%).

Delivery: [VERIFY: test center vs remote proctoring options in your region].

B) Domain Weights

Domain	Weight
1. Governance, Risk, Compliance	21%
2. Information Security Controls and Audit Management	20%
3. Security Program Management and Operations	21%
4. Information Security Core Competencies	19%
5. Strategic Planning, Finance, Procurement, and Third-Party Management	19%

C) Core Workflow (How the exam thinks)

- State the business goal and risk context before selecting controls.
- Set governance: authority, policy direction, roles, and decision rights.
- Identify and document risks (risk register); choose treatment and owner.
- Select controls and define measures (KPIs/KRIs) and testing approach.
- Run the program: projects, staffing, communications, and incident readiness.
- Report and assure: evidence, audit results, remediation tracking, and exec updates.

D) High-Yield Concepts

- Governance artifacts: charter, policies, standards, exceptions, and approvals.
- Risk framing: appetite vs tolerance; likelihood vs impact; residual risk.
- Compliance: map requirements to controls and maintain audit-ready evidence.
- Control management: design, implement, monitor, and improve control effectiveness.
- Audit management: risk-based plan, evidence quality, findings, and remediation.
- Program management: scope, budget, staffing, vendor coordination, and reporting.
- Security oversight: access control, network defense, encryption, and hardening decisions.
- Resilience: business impact analysis, BCP/DR governance, and testing cadence.
- Incident governance: escalation paths, evidence preservation, and lessons learned.
- Strategy and finance: roadmaps, budgeting, and procurement tradeoffs.

E) Common Traps

- Answering with a tool when the question is about authority, policy, or ownership.
- Treating every issue as high risk without likelihood and impact reasoning.
- Choosing an action without the required documentation, approval, or traceability.
- Confusing audits (evidence vs criteria) with assessments (what should be improved).
- Assuming a control is effective because it exists; look for monitoring and testing.
- Forgetting third-party exposure: contracts, right-to-audit, and ongoing reviews.

F) Cheat Sheet (Artifacts & decision cues)

- Risk register: scenario, likelihood, impact, treatment, residual risk, owner, review date.
- Controls: preventive, detective, corrective; administrative, technical, physical.
- Evidence chain: policy → procedure → record; current, approved, and used.
- Metrics: KPIs (outcomes), KRIs (risk signals), operational metrics (activity).
- Audit flow: plan, fieldwork, evidence, findings, response, remediation tracking.
- Third-party pack: due diligence, security addendum, SLA, incident notice terms, reviews.

G) Exam-Day Tactics

- Two-pass approach: answer fast wins; flag long scenarios for later.
- Eliminate wrong choices by spotting missing owner, missing evidence, or wrong scope.
- Prefer business-aligned answers with defined authority and measurable outcomes.
- For compliance items, choose the option that produces defensible documentation.
- Manage time: roughly one minute per question; protect a review buffer at the end.
- Re-read the stem on flagged items; many misses come from a single misread word.

H) 30-Minute Final Review Plan

- Use domain weights to set a 30-minute split across the five domains.
- Rehearse core artifacts: charter, risk register, control evidence, audit report, budget, vendor addendum.
- Refresh key pairs: appetite vs tolerance; KPI vs KRI; RTO vs RPO; preventive vs detective.
- Review one governance scenario and one audit scenario to anchor decision patterns.
- Set logistics and pacing: ID, platform check, quiet setup, and a plan for 150 questions.