Certified in Risk and Information Systems Control (CRISC) — One-Page Study Guide

BareMetalCyber.com | Cybersecurity Audio Academy
baremetalcyber.com/cybersecurity-audio-academy

A) Exam Snapshot

Issuer: ISACA | **Target level:** intermediate
Version: Job Practice Update effective 03 Nov 2025
Format: 150 multiple-choice questions (computer-based)
Time limit: 4 hours (240 minutes)
Scoring: scaled score (200-800); passing score 450

B) Domain Weights

Domain	Weight
1. Governance	26%
2. Risk Assessment	22%
3. Risk Response and Reporting	32%
4. Technology and Security	20%

C) Core Workflow (How the exam thinks)

- Frame the business objective and risk context (risk appetite, tolerance, key stakeholders).
- Define a risk scenario: asset/process, threat, vulnerability, triggering event, and business impact.
- Assess likelihood and impact using agreed criteria; consider existing controls and dependencies.
- Compare inherent risk vs residual risk; prioritize based on exposure and decision thresholds.
- Select a response option (mitigate, avoid, transfer/share, accept) and assign accountable owners.
- Design or refine controls; confirm control type (preventive, detective, corrective) and how effectiveness is measured.
- Monitor and report: KRIs and thresholds, control test results, issues/exceptions, and trend over time.
- Maintain evidence: risk register updates, approvals, and clear audit trail for decisions.

D) High-Yield Concepts

- Risk appetite vs risk tolerance (strategic direction vs acceptable variation for decisions).
- Inherent risk vs residual risk (before controls vs after controls).
- Risk scenario development (consistent structure improves comparability and reporting).
- Likelihood, impact, and exposure (how ratings are derived and justified).
- Qualitative vs quantitative assessment (when to use ordinal scales vs financial estimates).
- Control design vs control effectiveness (is it appropriate vs does it work in practice).
- KRI vs KPI vs KCI (risk signal vs performance vs control performance).
- Risk owner vs control owner (accountability for exposure vs accountability for operation).
- Risk treatment plan elements (actions, owners, dates, dependencies, success criteria).
- Third-party risk (shared responsibility, SLAs, assurance reports, and exit plans).
- Issue, finding, and exception management (tracking, remediation evidence, and acceptance).
- Governance cadence (committees, reporting frequency, escalation triggers).

E) Common Traps

- Jumping to a technical fix without confirming the business objective, risk criteria, and stakeholders.
- Confusing response options: choosing a control when the best answer is acceptance or avoidance (with approval).
- Ignoring existing controls when estimating likelihood/impact or when selecting the first response step.
- Mixing up KRIs with KPIs (performance metrics are not always risk indicators).
- Selecting an answer that lacks a named owner, due date, or approval evidence.
- Treating a heat map as the decision, rather than a visualization of agreed scoring criteria.
- Assuming third-party controls exist without an assurance artifact (report, attestation, contract clause).
- Choosing the most complex framework answer when a simpler governance/control artifact is sufficient.

F) Cheat Sheet (Artifacts to recognize)

- Risk scenario statement: *Condition* + *event* + *impact* (who/what is affected and how).
- Risk register minimum fields: scenario, owner, inherent/residual ratings, response, status, due dates.
- Response options: mitigate, avoid, transfer/share, accept (accept requires rationale + approval + review date).
- Control types: preventive, detective, corrective; map each to evidence you can review.
- KRI basics: threshold, trigger, trend, action owner; avoid vanity metrics.
- Artifacts to recognize: risk acceptance memo, exception log, remediation plan, control test results, assurance report.
- Third-party evidence: contract requirements and an assurance report/attestation tied to scope.

G) Exam-Day Tactics

- Time budget: about 1.6 minutes per question (240 minutes / 150 questions).
- First pass: answer the easy items quickly; mark uncertain items and move on.
- Read the last sentence first to identify what the question is truly asking.
- Map the scenario to the domain (governance, assessment, response/reporting, technology/security).
- Eliminate extremes and absolutes (always, never); prefer documented, risk-based decision logic.
- Pick the best next step with the least assumptions and the clearest evidence trail.
- Use final minutes to revisit marked items and confirm no unanswered questions remain.

H) 30-Minute Final Review Plan

- Re-scan domain weights and rehearse what each domain tests at a decision level.
- Refresh key pairs: appetite vs tolerance, inherent vs residual, KRI vs KPI vs KCI.
- Walk one sample scenario end-to-end: rating, response choice, owners, and reporting artifact.
- Do a short timed set (15-20 questions) and write one sentence on why each miss was wrong.
- Confirm exam logistics and rest plan (ID, check-in time, breaks, and pacing).

Source: official exam objectives & exam details. Quick review only; practice required. BareMetalCyber.com | https://baremetalcyber.com/cybersecurity-audio-academy