

Passing Standard: 70% estimated (450 on a 200-800 ISACA scaled score across 150 scored questions)

Format & Timing: 150 Scenario-Based Multiple Choice Questions. Total 4 hours. (PSI Services)

Testing Windows: Continuous testing year-round

1. OFFICIAL 2026 BLUEPRINT DOMAINS & WEIGHTINGS

CRISC-1: Governance (Organizational Governance, Risk Strategy)

Weight: 26% (39 Qs)

Organizational Strategy, Goals, Objectives, and Enterprise Governance Structure, Three Lines of Defense, Risk Ownership, Accountability, and RACI Matrix, Risk Appetite, Risk Tolerance, Risk Capacity, and Risk Culture, IT Risk Governance Frameworks (COBIT 2019, COSO ERM, ISO 31000) and Policies/Standards

CRISC-2: Risk Assessment (Risk Identification, Analysis, Evaluation)

Weight: 22% (33 Qs)

Risk Identification: Threat Modeling, Vulnerability Analysis, and Risk Scenario Development, Inherent Risk, Control Effectiveness Evaluation, and Residual Risk Determination, Qualitative vs. Quantitative Risk Analysis Methodologies (SLE, ARO, ALE, Monte Carlo, FAIR), Business Impact Analysis (BIA), Asset Valuation,

CRISC-3: Risk Response and Reporting (Risk Treatment, Controls Design)

Weight: 32% (48 Qs)

Risk Treatment Options (Avoid, Mitigate, Transfer/Share, Accept) and Cost-Benefit Analysis, Risk Action Plan Development, Prioritization, and Issue/Exception Management, Control Categories (Preventive, Detective, Corrective, Compensating, Deterrent) and Control Design/Implementation, Third-Party, Vendor, Supply

CRISC-4: Technology and Security (Architecture, Resilience)

Weight: 20% (30 Qs)

Enterprise Architecture, IT Operations, Change/Configuration Management, and SDLC Security Controls, Identity and Access Management (IAM), Encryption, Network Security, and Data Lifecycle Protection, Incident Response Management, Forensics Readiness, and Cyber Resilience, Business Continuity Planning

2. PRIMARY STATUTORY & REGULATORY AUTHORITIES TESTED

* ISACA Risk IT Framework & COBIT 2019 - Risk Governance (EDM03), Managed Risk (APO12), Three Li

Enterprise framework for governing, evaluating, and responding to IT risk aligned with business objectives

* NIST SP 800-30 Rev. 1, SP 800-37 Rev. 2 (RMF), and SP 800-53 Rev. 5 - Threat/Vulnerability/Imp

Federal and industry standards for conducting risk assessments, risk management lifecycle, and security/privacy control selection

* ISO/IEC 31000, ISO/IEC 27005 & COSO ERM Framework - Risk identification, qualitative vs. quant

International risk management principles, information security risk management, and enterprise risk integration

3. EXAMINER TRAPS & HIGH-YIELD PASS STRATEGY

Key Challenge: Aligning business risk appetite with technical control mitigation; distinguishing risk avoidance, mitigation, transfer, and acceptance in complex corporate scenarios.