CERTIFICATION BOARD

Certified Vulnerability Management Professional (CVMP)

Exam Objectives CVMP-001

About the exam

Item	Detail
Level	Intermediate
Number of questions	80. A performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions.
Delivery model	Computer adaptive in 3 stages of 28, 26, 26 questions. Your score on each stage selects the difficulty of the next, so no two candidates sit the same paper.
Time limit	120 minutes
Scoring	You need a score of 700 out of 900 to pass. Results are reported on a scale of 100 to 900, and 700 corresponds to answering 72% of the exam correctly. Harder questions carry more weight, so a score means the same thing on any route. Multiple-response items and PBQs are scored all or nothing.
Delivery	Online, fully proctored (webcam, microphone and screen).
Prerequisites	No formal prerequisite. Candidates do best with two years in security, systems or infrastructure work and 50 to 80 hours of study.
Retakes	No waiting period after a failed first attempt. Candidates pay the exam price each time they attempt the exam. See the CertLabz Certification Retake Policy at certlabz.com/certification-retake-policy.html
Validity	3 years. Renew with 50 CEUs per cycle and the $35 annual continuing-education fee, or by passing the current exam.
Language	English
Exam voucher	$149 for one sitting, valid 12 months. Bundles add the study guide ebook and the All Access plan.

Domain weights

Domain	Questions
D1 Vulnerability Management Foundations and Governance (13%)	10

D2 Asset Discovery and Inventory (15%)

	12
D3 Scanning and Assessment (17%)	14
D4 Analysis, Scoring and Prioritization (20%)	16
D5 Remediation, Mitigation and Verification (20%)	16
D6 Reporting, Metrics and Program (15%)	12
Total (100%)	**80**

Objectives by domain

Each objective may appear as knowledge, a scenario to judge, a circuit to trace or assemble, or a number to compute. Each form can carry up to 5 to 12 performance-based questions: drag-and-drop matching, sequencing and table completion, drawn fresh each attempt. The exam does not test any vendor's SDK syntax.

D1 Vulnerability Management Foundations and Governance — 13% — 10 questions

D1.1 The vulnerability management lifecycle versus a one-off assessment
D1.2 Vulnerability, threat and risk distinguished
D1.3 Policy, ownership, severity-based SLAs and executive sponsorship
D1.4 Scanning cadence and integration with change and ITSM
D1.5 Compliance drivers such as PCI DSS scanning requirements
D1.6 Continuous threat exposure management (CTEM) as the modern direction

D2 Asset Discovery and Inventory — 15% — 12 questions

D2.1 Inventory as the foundation; coverage gaps as blind spots
D2.2 Active, passive, agent, cloud-API and CMDB discovery combined
D2.3 Cloud, container and ephemeral asset discovery
D2.4 Ownership, business context and data-sensitivity classification
D2.5 Attack surface management and shadow assets
D2.6 Software inventory, SBOMs and deduplication across sources

D3 Scanning and Assessment — 17% — 14 questions

D3.1 Authenticated versus unauthenticated and agent-based scanning
D3.2 False positives and false negatives and how to reduce them
D3.3 Scan scheduling, throttling and impact on fragile systems
D3.4 Web application (DAST), container and cloud scanning
D3.5 Scan coverage as a critical metric; internal and external perspectives
D3.6 PCI ASV scans; scanning versus penetration testing

D4 Analysis, Scoring and Prioritization — 20% — 16 questions

D4.1 CVSS base, temporal and environmental metrics and their limits
D4.2 EPSS exploitation probability and the CISA KEV catalog
D4.3 SSVC decision-based categorization
D4.4 Exposure, reachability and business criticality in risk
D4.5 Threat intelligence and public exploit availability
D4.6 Risk-based prioritization and re-evaluation over time

D5 Remediation, Mitigation and Verification — 20% — 16 questions

D5.1 Remediation versus mitigation; compensating controls and virtual patching
D5.2 Risk-based SLAs, change windows and emergency changes
D5.3 Exceptions and risk acceptance done properly
D5.4 Patch testing, golden images and hardened baselines
D5.5 Verification by rescan; recurring and reopened findings
D5.6 Coordinating shared-component fixes and working with operations

D6 Reporting, Metrics and Program — 15% — 12 questions

D6.1 MTTR, SLA compliance, coverage and risk-weighted exposure
D6.2 Audience-tailored reporting and trend over snapshot
D6.3 Compliance evidence and defensible single-number reporting
D6.4 Integration with ticketing and CMDB for accurate reporting
D6.5 Incentives: risk reduced versus findings closed
D6.6 Using program data to improve the process

Continuing education

Renewal	Requirement
Validity	3 years from the date of issue
CEUs required per cycle	50
Annual CE fee	$35
Alternative to CEUs	Pass the current version of the exam before the expiry date

Qualifying activities

Activity	CEUs
CertLabz labs, PBQs, courses and SkillTracker assessments	1 CEU per hour, up to 25 per cycle
Other industry certifications earned or renewed	10 to 25 each, depending on level
Conferences, webinars and training	1 CEU per hour, up to 20 per cycle
Vulnerability management, security or systems work experience	3 per year, up to 9 per cycle
Teaching, mentoring, publishing or open-source contributions	Up to 15 per cycle
College courses in security, computing or information systems	10 per completed course

CertLabz Certification Retake Policy

- **No waiting period after a failed first attempt:** If you fail your first attempt at any CertLabz certification examination, CertLabz does not require any waiting period between the first and second attempt.
- **Once you pass, you cannot resit the same exam code:** A candidate who has passed an exam and achieved a certification cannot take that exam again under the same exam code without prior consent from CertLabz. You will need to wait until a new series of the exam is published before attempting to recertify by examination.
- **Beta examinations, one attempt only:** A CertLabz beta examination may be taken one time by each candidate.
- **Violations invalidate the attempt:** A test found to be in violation of this policy will be invalidated, and the candidate may be subject to a suspension period. Repeat violators will be permanently banned from the CertLabz Certification Program.
- **Every attempt is paid for:** Candidates must pay the exam price each time they attempt the exam. CertLabz does not offer free retests or discounts on retakes.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Objectives document CVMP-001.
https://certlabz.com/certifications/certified-vulnerability-management-professional.html