CERTLABZ CERTIFICATION BOARD

Certified Incident Response Professional (CIRP)

Exam Objectives CIRP-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 a SOC, security or systems role 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 Incident Response Foundations and Governance (15%)	12

D2 Preparation and Detection (16%)

	13
D3 Analysis and Investigation (20%)	16
D4 Containment, Eradication and Recovery (20%)	16
D5 Specific Incident Types (17%)	13
D6 Post-Incident, Communication and Legal (12%)	10
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 Incident Response Foundations and Governance — 15% — 12 questions

D1.1 The NIST SP 800-61 lifecycle and how phases connect
D1.2 Events versus incidents; severity and classification schemes
D1.3 The IR plan, playbooks, decision rights and pre-authorized authority
D1.4 CSIRT structure, roles and cross-functional stakeholders
D1.5 Metrics: dwell time, time to contain, time to recover, recurrence
D1.6 Retainers, insurance, tabletop exercises and out-of-band communication

D2 Preparation and Detection — 16% — 13 questions

D2.1 Asset inventory, logging baselines and central time-synced logs
D2.2 Detection sources: EDR, SIEM, users and external notification
D2.3 Triage, alert tuning, enrichment and reducing alert fatigue
D2.4 Escalation paths, on-call and the go-bag (jump kit)
D2.5 Threat intelligence in detection and log-retention versus dwell time
D2.6 Phishing-report handling and detection validation by emulation

D3 Analysis and Investigation — 20% — 16 questions

D3.1 Scoping: entry point, footprint, lateral movement and persistence
D3.2 Timeline reconstruction and cause and effect across sources
D3.3 Order of volatility, forensic imaging, write blockers and hashing
D3.4 Memory forensics, disk forensics and malware triage
D3.5 Indicators of compromise and pivoting to behaviours
D3.6 Avoiding tipping off the adversary; contemporaneous documentation

D4 Containment, Eradication and Recovery — 20% — 16 questions

D4.1 Short-term and long-term containment and their sequencing
D4.2 Eradicating malware, persistence and adversary access together
D4.3 Rebuild from known-good, close the exploited weakness
D4.4 Verified, clean, tested backups; RTO and RPO
D4.5 Validation, hardening and heightened monitoring on return
D4.6 Compensating controls and the availability-versus-risk decision

D5 Specific Incident Types — 17% — 13 questions

D5.1 Ransomware, double extortion and the pay decision
D5.2 Business email compromise and cloud account takeover
D5.3 Data breach, insider threat and evidence handling
D5.4 Web-application compromise and web shells
D5.5 Supply-chain compromise and destructive attacks
D5.6 DDoS response and federated-identity session revocation

D6 Post-Incident, Communication and Legal — 12% — 10 questions

D6.1 Lessons-learned reviews and tracked, owned actions
D6.2 Chain of custody and evidence admissibility
D6.3 Regulatory notification: GDPR 72 hours, breach and securities duties
D6.4 Engaging legal, privilege and law enforcement
D6.5 Coordinated external communication
D6.6 Updating detections, controls and the plan itself

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
Incident response, SOC or forensics 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 digital forensics	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 CIRP-001.
https://certlabz.com/certifications/certified-incident-response-professional.html