

**CERTLABZ****CERTIFICATION BOARD****CICSP-001**

Certified ICS Security Practitioner (CICSP)

Exam Objectives **CICSP-001**

About the exam

Item	Detail
Level	Advanced
Number of questions	120. 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 42, 39, 39 questions. Your score on each stage selects the difficulty of the next, so no two candidates sit the same paper.
Time limit	180 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 hands-on IT security or industrial/OT experience and 40 to 60 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 75 CEUs per cycle and the \$55 annual continuing-education fee, or by passing the current exam.
Language	English
Exam voucher	\$199 for one sitting, valid 12 months. Bundles add the study guide ebook and the All Access plan.

Domain weights

Domain	Questions
D1 ICS and OT Foundations (16%)	19
D2 ICS Protocols and Architecture (16%)	19
D3 Threats and Vulnerabilities (17%)	21

D4 Security Controls and Segmentation (17%)

	21
D5 Monitoring and Incident Response (17%)	20
D6 Standards, Risk and Governance (17%)	20
Total (100%)	120

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 ICS and OT Foundations

16% 19 questions

- D1.1 What ICS and OT are
- D1.2 PLCs, RTUs and SCADA
- D1.3 The Purdue model
- D1.4 IT versus OT differences
- D1.5 Safety and availability
- D1.6 Key terms

D2 ICS Protocols and Architecture

16% 19 questions

- D2.1 Modbus and DNP3
- D2.2 OPC and industrial protocols
- D2.3 Network architecture
- D2.4 Zones and conduits
- D2.5 Legacy systems
- D2.6 Wireless in OT

D3 Threats and Vulnerabilities

17% 21 questions

- D3.1 ICS threat landscape
- D3.2 Common vulnerabilities
- D3.3 Attack techniques
- D3.4 Malware in OT
- D3.5 Insider and supply chain
- D3.6 Threat intelligence

D4 Security Controls and Segmentation

17% 21 questions

- D4.1 Network segmentation
- D4.2 Firewalls and the DMZ
- D4.3 Access control
- D4.4 Hardening
- D4.5 Secure remote access
- D4.6 Patch and change management

D5 Monitoring and Incident Response

17% 20 questions

- D5.1 OT monitoring
- D5.2 Anomaly detection
- D5.3 Logging and visibility
- D5.4 Incident response for OT
- D5.5 Recovery and continuity
- D5.6 Tabletop exercises

D6 Standards, Risk and Governance

17% 20 questions

- D6.1 IEC 62443
- D6.2 NIST and NERC CIP
- D6.3 Risk assessment
- D6.4 Governance and policy
- D6.5 Compliance
- D6.6 Vendor and asset management

Continuing education

Renewal	Requirement
Validity	3 years from the date of issue
CEUs required per cycle	75
Annual CE fee	\$55
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
ICS/OT or cybersecurity work experience	3 per year, up to 9 per cycle
Teaching, mentoring, publishing or community contributions	Up to 15 per cycle
College courses in computing, engineering or security	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 CICSP-001.
<https://certlabz.com/certifications/certified-ics-security-practitioner.html>