

**CERTLABZ****CERTIFICATION BOARD****COSE-001**

Certified OT Security Engineer (COSE)

Exam Objectives COSE-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 three years in industrial automation, networking or security work and 60 to 100 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 OT, ICS and Control System Fundamentals (16%)	19
D2 Threats, Risk and Standards (16%)	19
D3 Network Architecture and Segmentation (17%)	21

D4 Asset, Vulnerability and Patch Management (17%)

	21
D5 Monitoring, Detection and Incident Response (17%)	20
D6 Governance, Safety and Secure Operations (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 OT, ICS and Control System Fundamentals

16% 19 questions

- D1.1 OT versus IT priorities: safety, availability, integrity
- D1.2 PLCs, RTUs, HMIs, SCADA, DCS, historians, engineering workstations
- D1.3 The Purdue reference model
- D1.4 Safety instrumented systems
- D1.5 Industrial protocols: Modbus, DNP3, OPC UA, PROFINET, EtherNet/IP
- D1.6 Long lifecycles, legacy platforms and fragile devices

D2 Threats, Risk and Standards

16% 19 questions

- D2.1 Stuxnet, TRITON, Industroyer and IT-driven OT shutdowns
- D2.2 MITRE ATT&CK for ICS and impact categories
- D2.3 IEC 62443 zones, conduits and security levels
- D2.4 NIST SP 800-82 and NERC CIP at a high level
- D2.5 Consequence-driven risk assessment
- D2.6 Initial access paths: remote access, transient devices, media

D3 Network Architecture and Segmentation

17% 21 questions

- D3.1 Industrial DMZ and brokered flows
- D3.2 Zoning, default-deny conduits and protocol-aware firewalls
- D3.3 Data diodes and unidirectional gateways
- D3.4 Brokered, monitored vendor remote access
- D3.5 Wireless, cellular and cloud connectivity
- D3.6 Dual-homed hosts and porous air gaps

D4 Asset, Vulnerability and Patch Management

17% 21 questions

- D4.1 Passive discovery and the OT asset record
- D4.2 ICS advisories and vendor bulletins
- D4.3 Consequence-based prioritization beyond CVSS
- D4.4 Vendor-approved patching in maintenance windows
- D4.5 Compensating controls and unsupported hosts
- D4.6 Baselines, allow-listing, firmware integrity, default credentials

D5 Monitoring, Detection and Incident Response

17% 20 questions

- D5.1 Passive network monitoring and baselining
- D5.2 Protocol anomaly and command detection
- D5.3 Safe containment coordinated with operations
- D5.4 Evidence: captures, historian data, workstation logs
- D5.5 Verified logic backups and recovery
- D5.6 One-way SIEM integration and tabletop exercises

D6 Governance, Safety and Secure Operations

17% 20 questions

- D6.1 Cross-functional ownership and Management of Change
- D6.2 Safety-system isolation and key switches
- D6.3 Supply chain, integrators and vendor governance
- D6.4 Physical security as a cyber control
- D6.5 Secure by design in new projects
- D6.6 OT identity separation, training and metrics

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
OT, ICS or industrial security 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 engineering, security or computing	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 COSE-001.
<https://certlabz.com/certifications/certified-ot-security-engineer.html>