CERTLABZ CERTIFICATION BOARD

Certified ICS Security Practitioner (CICSP)

Ten Sample Questions

These ten questions are written at the difficulty of the live exam. Six carry a figure, a data table, a configuration or a code listing; four are plain scenario questions, as on the live paper. Every one is a scenario a working ICS security practitioner would meet, and none of them appears in the live question bank.

The live exam is multistage adaptive: how you score on one stage selects the difficulty of the next, so no two candidates sit the same paper. It is a performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions, which means you build, sequence or complete something rather than only choosing from a list. Answers and full explanations follow each question here; the live exam does not disclose item-level answers.

Question 1

Domain 1: ICS and OT Foundations

DATA

Emma Wilson reviews the Purdue model levels, with one function missing.

Level	Function
Level 0	Field sensors and actuators
Level 1	(to choose)
Level 2	Area supervisory control
Level 3	Site operations

Table 1.1 Purdue model levels.

What belongs at Level 1?

A. Enterprise IT servers
B. Field sensors only
C. Basic control (PLCs)
D. Corporate email hosts

Correct answer: C
In the Purdue model, Level 1 holds the basic control devices such as programmable logic controllers that drive the process. Level 0 is the field sensors and actuators, while enterprise servers and corporate email sit in the upper business levels.

Question 2 — Domain 2: ICS Protocols and Architecture — DATA

James Carter maps each industrial protocol to its purpose, with one purpose missing.

Protocol	Purpose
Modbus TCP	(to choose)
DNP3	Utility SCADA telemetry
OPC UA	Secure data exchange
EtherNet/IP	Industrial device control

Table 2.1 Protocols and purpose.

What is Modbus TCP used for?

A. Read holding registers
B. Serve encrypted webmail
C. Resolve host addresses
D. Distribute system time

Correct answer: A
Modbus TCP is a simple industrial protocol used to read and write device registers and coils, so reading holding registers is its purpose. It does not serve webmail, resolve host addresses, or distribute system time.

Question 3 — Domain 3: Threats and Vulnerabilities — CONFIG

Olivia Davis reviews the scan findings for a plant controller.

```
asset    plc-line-3
firmware v2.1 (2016)
telnet   open, no auth
https    enabled
syslog   forwarding on
```

Listing 3.1 Asset scan findings.

Which finding is the most serious remote exposure?

A. Firmware is dated 2016
B. Telnet has no auth
C. HTTPS stays enabled
D. Syslog is forwarding

Correct answer: B
An open telnet service with no authentication lets anyone on the network take control of the device remotely, so it is the most serious exposure. Dated firmware, an enabled web interface, and syslog forwarding are lesser concerns that do not grant instant unauthenticated access.

Question 4

Domain 4: Security Controls and Segmentation

CONFIG

Liam Anderson reviews the firewall rules between plant zones, where one rule is far too permissive.

```
L3 to L2   allow 502
L2 to L1   allow 44818
any to any allow all
L4 to DMZ  allow 443
```

Listing 4.1 Firewall rules between zones.

Which rule breaks the zone segmentation?

A. L2 to L1 EtherNet rule
B. L3 to L2 Modbus rule
C. L4 to DMZ HTTPS rule
D. Any to any allow rule

Correct answer: D
A rule that allows any source to any destination collapses the boundary between zones and defeats segmentation. The Modbus, EtherNet, and HTTPS rules each permit a single expected flow between defined levels, which is the intended least privilege pattern.

Question 5

Domain 5: Monitoring and Incident Response

DATA

Ava Thompson maps each monitoring source to what it detects, with one entry missing.

Source	Detects
Network IDS	(to choose)
Host logs	Local login events
Asset inventory	Rogue new devices
PLC change log	Logic downloads

Table 5.1 Monitoring sources.

What does the network IDS mainly detect?

A. Physical door access
B. Payroll data changes
C. Odd network traffic

D Building temperature

Correct answer: C
A network intrusion detection system watches traffic and flags unusual or malicious patterns, so odd network traffic is what it mainly detects. Physical door access, payroll changes, and building temperature come from other systems, not a network sensor.

Question 6

Domain 6: Standards, Risk and Governance

DATA

David Brown maps each standard to its focus, with one focus missing.

Standard	Focus
IEC 62443	(to choose)
NIST SP 800-82	ICS security guidance
ISO 27001	Information security
NERC CIP	Bulk power reliability

Table 6.1 Standards and focus.

What is the focus of IEC 62443?

A IACS security zones
B Food safety auditing
C Payment card handling
D Medical device labels

Correct answer: A
IEC 62443 is the standard family for industrial automation and control system security, built around zones, conduits, and a secure lifecycle. It does not cover food safety, payment cards, or medical device labeling, which fall under other standards.

Question 7

Domain 1: ICS and OT Foundations

A team applies its usual IT patch approach and forces immediate reboots on a running production line, tripping the process. What ICS priority did the team ignore?

A Data confidentiality
B Fast patch cycles
C Encryption strength
D System availability

Correct answer: D
Control systems place safety and availability first, so forcing immediate reboots on a running line ignores system availability. Confidentiality and encryption still matter, but they do not outrank keeping the process running safely, and faster patch cycles are not an ICS priority in themselves.

Question 8 Domain 3: Threats and Vulnerabilities

An attacker emails an engineer a crafted document to gain a foothold on the workstation that programs the controllers. What is this initial technique?

A. Physical tailgating
B. Spear phishing
C. Cable tapping
D. Radio jamming

Correct answer: B
Emailing a crafted document to an engineer to gain a foothold on the workstation that programs the controllers is spear phishing, a targeted social attack. Tailgating, cable tapping, and radio jamming are physical or signal attacks that do not match the email based method described.

Question 9 Domain 4: Security Controls and Segmentation

The enterprise needs read access to plant data, but direct connections from Level 4 into the control network are unsafe. Where should the shared historian sit?

A. Inside Level 1
B. On the PLC itself
C. In the IT/OT DMZ
D. On the open internet

Correct answer: C
A shared historian belongs in the IT/OT demilitarized zone, where enterprise users can read plant data without a direct path into the control network. Placing it inside Level 1, on a controller, or on the open internet would either expose the process or break the segmentation boundary.

Question 10 Domain 5: Monitoring and Incident Response

Malware is found spreading on the control network during production. What should the ICS incident response prioritize first?

A. Keep the process safe
B. Wipe every device now
C. Post details publicly
D. Ignore until Monday

Correct answer: A
Incident response in a control environment prioritizes keeping the process safe before aggressive containment, because rash actions can trip equipment or endanger people. Wiping every device at once, disclosing details publicly, or waiting until Monday would raise risk rather than reduce it.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Companion to objectives document CICSP-001. https://certlabz.com/certifications/certified-ics-security-practitioner.html