CERTLABZ CERTIFICATION BOARD

# Certified Security Awareness Trainer (CSAT)

## 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 security awareness trainer 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: Security Awareness Foundations

DATA

Sarah Miller maps each security goal to what it protects, with one goal missing.

| Goal | Protects |
|---|---|
| Confidentiality | Keeps data private |
| (to choose) | Keeps data accurate |
| Availability | Keeps data reachable |
| Accountability | Ties actions to users |

Table 1.1 Security goals and meaning.

Which goal fills the blank?

A. Integrity
B. Secrecy
C. Backup
D. Encryption

**Correct answer: A**

Integrity is the goal that keeps data accurate and unaltered, so it fills the blank. Secrecy overlaps with confidentiality, while backup and encryption are controls rather than the core goal named here.

## Question 2 — Domain 2: Human Risk and Social Engineering — DATA

James Carter lists common attacker tactics against the cue each one relies on.

| Tactic | Relies on |
|---|---|
| Pretexting | A believable story |
| Baiting | Curiosity or greed |
| Tailgating | (to choose) |
| Quid pro quo | Offer of a favour |

Table 2.1 Tactics and their cues.

What does tailgating rely on?

- A. A fake invoice
- B. A held door
- C. A prize email
- D. A phone survey

**Correct answer: B**
Tailgating relies on following an authorised person through a held door to enter a restricted area. A fake invoice and prize email are digital lures, and a phone survey is a pretext, not physical entry.

## Question 3 — Domain 3: Building an Awareness Program — DATA

Emma Wilson drafts a program roadmap, with the first step left blank.

| Order | Step |
|---|---|
| 1 | (to choose) |
| 2 | Set clear goals |
| 3 | Plan the topics |
| 4 | Measure results |

Table 3.1 Program build order.

Which step comes first?

- A. Buy new tools
- B. Assess the risks
- C. Print posters
- D. Reward top staff

**Correct answer: B**
Assessing the risks comes first so goals and topics target the real gaps the workforce faces. Buying tools, printing posters, or rewarding staff are later actions that should follow a clear risk picture.

## Question 4 — Domain 4: Training Delivery and Engagement — CONFIG

David Brown reviews a short training policy snippet used at onboarding.

```
New hires   finish training week one
All staff   refresh every year
Format      short modules plus quiz
Records     kept for two years
```

Listing 4.1 The training policy snippet.

Which practice keeps learners most engaged?

A. One long yearly class
B. Short modules plus quiz
C. Reading only, no quiz
D. Slides with no recap

**Correct answer: B**
Short modules paired with a quick quiz keep attention and help learners retain each point. One long class, reading with no check, or slides without recap tend to lose the audience and test little.

## Question 5 — Domain 5: Phishing Simulations and Testing — CONFIG

Olivia Davis studies the header of a simulated phishing email.

```
From:    IT-Helpdesk <help@1t-support.co>
To:      staff@company.com
Subject: Urgent: reset your password now
Reply-To: no-reply@mail-secure.ru
```

Listing 5.1 The email header.

Which clue best signals a phishing attempt?

A. It has a subject
B. It went to staff
C. Odd sender domain
D. It uses email

**Correct answer: C**
The odd sender domain with a number in place of a letter, plus a foreign reply-to address, are strong phishing signals. Having a subject, reaching staff, or simply using email are normal traits of any message.

## Question 6

Domain 6: Metrics, Culture and Compliance

DATA

Ava Thompson reviews last quarter metrics to judge the program.

| Metric | Value |
| --- | --- |
| Training completion | 96 percent |
| Phishing click rate | 4 percent |
| Reports of phishing | Rising |
| Repeat clickers | Falling |

Table 6.1 Quarterly program metrics.

Which trend best shows a healthy security culture?

A. More repeat clickers
B. Lower report rate
C. Rising phish reports
D. Skipped training

**Correct answer: C**
Rising reports of phishing show staff notice and flag suspicious email, a sign of a healthy culture. More repeat clickers, fewer reports, or skipped training all point the wrong way for a maturing program.

## Question 7

Domain 1: Security Awareness Foundations

A new employee thinks security is only the job of the IT team and ignores the training. What idea best corrects this view?

A. Only IT is at risk
B. Security is shared
C. Tools stop all threats
D. Rules waste time

**Correct answer: B**
Security is a shared responsibility, since every person handles data and can be targeted by attackers. Believing only IT is at risk, that tools stop everything, or that rules waste time leaves the human layer exposed.

## Question 8 Domain 2: Human Risk and Social Engineering

A caller claims to be the chief executive and pressures a clerk to move funds at once, warning her not to check with anyone. What should the clerk do?

- A Send the funds fast
- B Verify through a channel
- C Keep it a secret
- D Reply to the caller

**Correct answer: B**
Verifying the request through a known separate channel exposes this classic urgency and authority scam before any money moves. Sending funds, keeping it secret, or trusting the same call all play into the attacker plan.

## Question 9 Domain 4: Training Delivery and Engagement

Staff say the yearly training feels dull and unrelated to their daily work, so few pay attention. What change best raises engagement?

- A Make it longer
- B Use role-based content
- C Add more legal text
- D Remove the quiz

**Correct answer: B**
Role-based content ties lessons to the real tasks and risks each group faces, which lifts attention and relevance. Longer sessions, more legal text, or dropping the quiz do not make the material feel useful to the learner.

## Question 10 Domain 6: Metrics, Culture and Compliance

A leader wants one number to prove the awareness program works and points only to the training completion rate. Why is that measure alone weak?

- A It is hard to track
- B It shows only sign-off
- C It costs too much
- D It cannot be reported

**Correct answer: B**
Completion shows only that people finished a module, not that behaviour changed, so it reflects sign-off rather than real risk reduction. It is easy to track and report, so cost and tracking are not the true weakness here.

CSAT-001. https://certlabz.com/certifications/certified-security-awareness-trainer.html