CERTLABZ CERTIFICATION BOARD

Certified Digital Asset Custody Specialist (CDACS)

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 digital asset custody specialist 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: Custody Foundations — DATA

Emma Wilson matches each storage type to its tradeoff.

Storage	Tradeoff
Hot wallet	(to choose)
Cold storage	(to choose)
Warm wallet	(to choose)
Self-custody	(to choose)

Table 1.1 Storage tradeoffs.

Which set of tradeoffs is correct?

A. Offline and safest but slow, online and fast but exposed, a middle ground, and the user holds the keys, in the order shown.

B. Online and fast but more exposed, offline and safest but slower, a balanced middle ground, and the user holds the keys directly.

C. The user holds the keys, a balanced middle ground, offline and safest but slower, and online and fast but exposed, in order.

D. A balanced middle ground, online and fast but exposed, the user holds the keys, and offline and safest but slower, in order.

Correct answer: B
A hot wallet is online and fast but more exposed, cold storage is offline and safest but slower, a warm wallet is a balanced middle ground, and self-custody means the user holds the keys directly. Only option B pairs each storage type with its tradeoff.

Question 2 — Domain 2: Key Management — CONFIG

James Carter reviews a key-management design note.

```
signing        : requires 3 of 5 approvers
key storage    : hardware security modules
no single      : person can move funds alone
backup         : sharded and geographically split
```

Listing 2.1 Design note.

What principle does this design primarily enforce?

A. Single-person efficiency, because letting one approver move funds quickly is the main goal of a custody signing design.

B. No single point of failure, since multiple approvers, HSMs and split backups mean no one person or device can move funds alone.

C. Public transparency, because the design publishes the approver keys so anyone can verify who signed each transaction.

D. Maximum speed, because requiring several approvers and hardware modules is the fastest possible way to move client funds.

Correct answer: B
Requiring multiple approvers, storing keys in HSMs and sharding backups all ensure that no single person or device can move funds, eliminating single points of failure. It is not about single-person efficiency, publishing keys, or maximizing speed.

Question 3 — Domain 4: Security and Threats — DATA

Olivia Davis matches each threat to its control.

Threat	Control
Rogue insider moves funds	(to choose)
Phishing an operator	(to choose)
Compromised vendor tool	(to choose)
Physical theft of a device	(to choose)

Table 3.1 Threats and controls.

Which set of controls is correct?

A. Supply-chain review, separation of duties, secure facilities, and training with strong authentication, in the order shown here.

B. Separation of duties, training and strong authentication, supply-chain review, and secure facilities with tamper protection.

C. Secure facilities, supply-chain review, separation of duties, and training with authentication, in the order shown in the table.

D. Training and authentication, secure facilities, separation of duties, and supply-chain review, in the order shown in the table.

Correct answer: B
A rogue insider is controlled by separation of duties, phishing by training and strong authentication, a compromised vendor tool by supply-chain review, and physical theft by secure facilities with tamper protection. Only option B pairs each threat with its control.

Question 4

Domain 6: Operations, Recovery and Governance

CONFIG

Liam Anderson lists the steps to handle a suspected key compromise, out of order.

```
A. Rotate keys and restore from secure backup
B. Detect and confirm the suspected compromise
C. Contain by freezing affected operations
D. Investigate scope and affected assets
```

Listing 4.1 Response steps.

What is the correct order?

A. A, then C, then B, then D, rotating keys and freezing operations before the compromise has been detected or confirmed at all.

B. B, then C, then D, then A, detecting and confirming, containing by freezing, investigating scope, then rotating keys and restoring.

C. D, then A, then B, then C, investigating and rotating before the compromise is detected or the affected operations are frozen.

D. C, then B, then D, then A, freezing operations before the compromise has been detected or confirmed as real in the first place.

Correct answer: B
The response is: detect and confirm the compromise, contain by freezing affected operations, investigate scope and affected assets, then rotate keys and restore from secure backup. The other orders rotate keys or freeze before the compromise is detected and confirmed.

Question 5

Domain 5: Compliance and Controls

DATA

Ava Thompson matches each control to what it demonstrates.

Control	Demonstrates
Proof of reserves	(to choose)
Segregation of client assets	(to choose)
Independent audit	(to choose)
Insurance	(to choose)

Table 5.1 Compliance controls.

Which set is correct?

A. Client funds kept apart from firm funds, that assets exist to back liabilities, external verification, and loss cover, in order.

B. That assets exist to back client liabilities, client funds kept apart from firm funds, external verification, and cover for losses.

C. External verification, cover for losses, that assets exist to back liabilities, and client funds kept apart, in the order shown.

D. Cover for losses, external verification, client funds kept apart, and that assets exist to back liabilities, in the order shown.

Correct answer: B
Proof of reserves demonstrates that assets exist to back client liabilities, segregation keeps client funds apart from firm funds, an independent audit provides external verification, and insurance provides cover for losses. Only option B maps each control to what it demonstrates.

Question 6

Domain 3: Wallet Architecture and Operations

DATA

A custody team reviews signing-operation safeguards.

Safeguard	Purpose
Address whitelisting	Limit where funds can go
Withdrawal limits	Cap exposure per period
Dual approval	No single approver signs
Segregated accounts	Keep client assets apart

Table 6.1 Signing safeguards.

What is the best summary of safe signing operations?

A. Let any single operator sign any withdrawal to any address instantly, because speed is the only real goal of custody operations.

B. Constrain where funds go, cap exposure, require multiple approvers, and keep client assets segregated, so no single action is unchecked.

C. Remove all limits and approvals once a client is verified, since verification alone makes every later withdrawal automatically safe.

D Publish the signing keys to clients, so that clients can co-sign their own withdrawals directly without any custody controls.

Correct answer: B
Safe signing constrains destinations with whitelisting, caps exposure with withdrawal limits, requires multiple approvers with dual approval, and keeps client assets segregated, so no single action is unchecked. Instant single-operator signing, removing controls after verification, or publishing keys all defeat custody.

Question 7 Domain 1: Custody Foundations

A client asks why a custodian keeps most assets in cold storage rather than all in a fast hot wallet. How do you explain it?

A There is no reason, because keeping everything in a hot wallet is the safest and most standard custody arrangement available.

B Cold storage keeps most assets offline and hardest to steal, while a smaller hot wallet handles day-to-day withdrawals.

C Cold storage is only for assets the custodian plans to discard, so keeping most funds there means most funds are unwanted.

D Hot wallets are safer than cold storage, so the custodian is actually taking on more risk by using cold storage at all.

Correct answer: B
Custodians keep most assets in cold storage because being offline makes them hardest to steal, while a smaller hot wallet covers day-to-day withdrawals. Keeping everything hot maximizes exposure, cold storage is not for discarded assets, and hot wallets are more exposed, not safer.

Question 8 Domain 2: Key Management

A custody startup stores the single private key for all client funds on one encrypted laptop. Why is this unacceptable, and the fix?

A It is acceptable, because encrypting the laptop removes every risk of losing or exposing the single key for all client funds.

B A single key is a catastrophic single point of failure; use multisig or MPC with HSMs so no one key or device controls the funds.

C The only issue is disk space, so moving the key to a larger drive resolves the concern about holding all client funds on it.

D The fix is to memorize the key and delete the file, so that no copy of the client key exists anywhere at all afterward.

Correct answer: B
A single key on one device is a catastrophic single point of failure: its theft or loss compromises all client funds. The fix is multisig or MPC combined with HSMs so no single key or device controls the funds. Encryption alone, more disk space, or memorizing and deleting the key do not remove that risk.

Question 9 Domain 5: Compliance and Controls

Why do institutional clients and regulators expect segregation of client assets and proof of reserves from a custodian?

A. They do not; mixing client and firm funds and keeping reserves private is the expected standard for a digital asset custodian.

B. Because segregation keeps client assets safe from firm liabilities and proof of reserves shows the assets truly back client balances.

C. Because segregation lets the custodian trade client funds freely, and proof of reserves is only a marketing exercise with no substance.

D. Because both controls exist solely to increase fees, providing no protection to clients or assurance to regulators in practice.

Correct answer: B
Segregation keeps client assets separate from firm liabilities so they are protected if the firm fails, and proof of reserves demonstrates that held assets truly back client balances. Mixing funds is not the standard, segregation prevents rather than enables trading client funds, and these controls provide real protection, not just fees.

Question 10 Domain 6: Operations, Recovery and Governance

A custodian has never tested its disaster-recovery and key-restoration procedures because nothing has gone wrong yet. What is the sound guidance?

A. No testing is needed, because a procedure that has been written down will always work correctly the first time it is used.

B. Test recovery and key restoration regularly, because an untested procedure often fails exactly when it is needed most in a crisis.

C. Testing recovery is dangerous and should never be done, since exercising the procedure is what causes real outages to occur.

D. Wait for a real incident to test the procedure, because an actual disaster is the only valid way to confirm recovery works.

Correct answer: B
Recovery and key-restoration procedures should be tested regularly, because an untested procedure frequently fails at the moment it is needed. Assuming a written plan works, refusing to test, or waiting for a real disaster to find out all leave the custodian unable to recover when it matters.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Companion to objectives document CDACS-001. https://certlabz.com/certifications/certified-digital-asset-custody-specialist.html