CRYPTOCURRENCY SECURITY STANDARD

CCSSA v9.0: Exam Scenario F

You are auditing a centralized exchange that serves a wide range of clients, and is certified under ISO/IEC 27001.

During your audit, you meet virtually with the exchange's Director of Custody Operations, who explains that the exchange uses a tiered custody pool model. Assets are allocated into three tiers: an operational pool for high-frequency withdrawals, a settlement pool for scheduled transactions, and long-term vault cold storage. Withdrawals from the operational pool are automated within set thresholds, while settlement and vault pools require progressively higher levels of multi-party review and sign-off.

Key material is generated using Hash_DRBG with 256 bits and the wallet is generated using MPC. The scheme is configured as a 4-of-7 threshold. Key shares are distributed in real time across multiple MPC nodes, with one node operated by a certified Level 3 CCSS Qualified Service Provider as the third-party custodian. Encrypted backup shares, protected with SHA-256, digital signatures, and secure logging, are on an HSM within an access-controlled vault. Audit logs are continuously monitored, and the shares are inspected quarterly to confirm they have not been altered.

You interview several key holders that are internal executives, but do not interview the external service provider as they are CCSS certified at Level 3. Each of the key holders you interview describes clear responsibilities, including approved communication channels. The exchange's Key Compromise Policy outlines these roles and mandates live compromise response drills once per year. Records and attendance logs confirm that the exercises have been conducted as scheduled and documented.

Policy documentation is centrally stored in a version-controlled repository with restricted access. Documents state that sanitization and destruction of media holding key material conform to SP 227-B7. The policy and procedure documentation is read and acknowledged by all staff who have access to key material. Documentation includes policies on governance, key management, smart contract deployment, incident response, and vendor oversight. Each document is electronically signed by a senior executive and marked with its last review date. Committee minutes confirm that the Risk and Compliance Board, chaired by an independent director, meets every two years to review the threat model. The threat model, aligned with ISO/IEC 27005, incorporates both internal audit findings and intelligence feeds from external

partners. Risk treatment plans are tracked in a dedicated system, each with an assigned owner and scheduled verification.

The exchange's smart contract program supports the operation of staking pools and structured lending for institutional clients. Developers explain that every contract is subject to a third-party audit and code review prior to deployment. The audit reports are stored alongside deployment records, and findings are tracked through a remediation system until all issues are confirmed as resolved. In addition, the exchange subscribes to a continuous smart contract monitoring service that scans for abnormal on-chain behavior and compliance risks.

Monitoring and incident response are managed by a globally distributed Security Operations Center. Analysts monitor centralized logs signed for integrity, backed up in near-real time to separate secure environments. Alerts are generated for anomalies such as unusual trading activity and unexpected key access attempts. Response procedures are documented, and staff demonstrate the escalation process during your review.

The exchange also undergoes vulnerability testing and standard penetration testing annually. Reports cover both infrastructure and smart contract systems, with remediation actions tracked to closure in the same risk system reviewed by the board.

NOTE: This exam scenario is designed to test your ability to analyze and apply the CCSS based on the information provided. Please keep the following in mind:

- *Only consider the evidence described in the scenario.*
    - *In some cases, there is intentionally not enough information to make a determination.*
    - *If something is not mentioned, you should not assume it exists.*
- *The purpose of these scenarios is to assess your ability to map given facts to the CCSS, not to evaluate the adequacy or quality of testing procedures.*
- *While we recognize auditors are trained to be precise and detail-oriented, for the purpose of this exam, focus only on what is explicitly presented in the scenario.*