CCSSA v9.0: Exam Scenario E

A mid-sized firm offers custodial services for institutional cryptocurrency investors. The company has grown quickly over the past three years, moving from a small in-house operation to managing billions of dollars' worth of assets across multiple digital asset classes. The firm serves a mix of hedge funds, family offices, and a few regulated investment trusts.

The core of the firm's system is a hybrid custody model. Hot wallets are used for client deposits and smaller withdrawals, while the majority of assets are held in cold storage. Key material for cold storage wallets is generated inside a dedicated restricted-access HSM. The HSM requires dual authorization to access. The generation mechanism for key material uses Dual_EC_DRBG. Key material is split into a 3-of-5 threshold scheme. Each share is stored individually and geographically separate. All the key holders and anyone who could impact the security of key generation, management, or usage had reference checks before they got access to any key material or operations related to key material.

For hot wallet operations, the firm relies on a 2-of-3 multi-signer system. Transactions are initiated by the client services team, and reviewed for funds destinations and amounts through approved communication channels and executed by key holders. Multi-factor authentication is enforced at every level of access to key material. Daily transfer limits are configured and alerts are triggered if thresholds are exceeded.

System logs are collected on a centralized logging server, backed up nightly to a separate environment, and monitored by the security operations team. Alerts for anomalous behavior, such as unusual transaction volumes or unauthorized login attempts, are triaged in real time. In addition, the firm subscribes to a blockchain monitoring service that flags suspicious activity like double-spend attempts or withdrawals to high-risk addresses.

The Chief Risk Officer signs off annually on the firm's security posture and risk model and formally acknowledges their responsibilities in writing. The firm maintains a threat model that is updated semi-annually or when significant changes are made to the custody platform. The risk management program used is based on NIST SP 800-37.

Key compromise preparedness has been a priority for the firm. A Key Compromise Policy (KCP) is formally documented, listing all operational and backup keys, roles, procedures, and secure approved communication channels enabled with 2FA. The firm conducts annual training exercises to rehearse compromise scenarios, documenting outcomes and adjusting policies as needed. Any changes to the people, processes, or technology triggers a test of their KCP and a new analysis of their threat model.

The firm commissions an independent third-party security audit every year, including penetration tests on its web portal. Findings are tracked in a remediation system until verified as resolved.

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.*