Exam Scenario C

A new cryptocurrency-based hedge fund has reached out to you to perform an audit for compliance with the CryptoCurrency Security Standard (CCSS).

The hedge fund has been operating in a conservative stealth mode while they continue to refine their financial offerings before launching to the public. The hedge fund managers have an extensive background in cryptocurrency investing, and have seen what does and doesn't work in the marketplace due to their prior experience.

Since the hedge fund is good at managing finances, and not security, they had the foresight to hire an external cryptocurrency security firm to help with architecting their information systems. The security firm provided the hedge fund with a peer-reviewed "seed generation kit" consisting of instructions on how to airgap a new laptop, how to generate a mnemonic seed on that laptop using a True Random Number Generator, and how to securely store and transmit key information. While researching the number generator that was referenced in the seed generation kit, you see that it previously passed Crypt-X and DIEHARD statistical tests. The hedge fund followed the seed generation instructions and each hedge fund manager proceeded to create their own keys from the newly-generated seed. The seed was then stored on two AES-256 encrypted USB thumb drives which were individually sealed in signed and dated tamper-evident bags. One of the sealed bags remains in a lockbox at the hedge fund office, while the other was sent to an offshore entity to be stored in a keyed safe for backup purposes. Both the office and offshore entity employ building access policies such as badges and PIN codes to enter the building. When checking the safe model numbers that were used, you can see that they are fireproof, shockproof, waterproof, and have a degree of protection from electromagnetic pulses.

On a day to day basis each hedge fund manager uses their own key and wallet to manage their customers' portfolios. The key is one of many that is used to sign multi-signature transactions. Policies are in place that state that no keys shall be shared amongst managers, and each manager's key should only be used on that manager's desktop computer in the office. Approved Communication Channels are used during execution. Should a key be lost or compromised, procedures are in place to ensure proper key revocation and regeneration. The hedge fund managers were trained to use new addresses while verifying all amounts prior to signing transactions.

As part of an annual company task, all procedures and processes are tested for effectiveness. Updates to these policies and procedures take place wherever inefficiencies are identified

during quarterly review and testing. Some of these policies include a data classification policy, a data sanitization policy, and identification of all permissions and roles within the system.

Since the hedge fund is in stealth mode, they've yet to do an annual penetration test -- although the external cryptocurrency security firm that helped with the seed generation process did an initial security audit and found no issues at that time.