Exam Scenario B

A decentralized non-custodial cryptocurrency exchange has reached out to you to perform an audit so they may pursue a level of CryptoCurrency Security Standard (CCSS) compliance. Since the exchange is decentralized, the need for secrecy provides a challenge for reviewing certain aspects of the CCSS.

The exchange is located and operates in another country, and not much is known publicly about the executive staff and owner. As part of your audit documentation gathering, the "Security Engineer" for the decentralized exchange has provided you with some sanitized infrastructure diagrams and meeting notes from when the exchange was originally created. Since the exchange was recently compromised, they express some nervousness about the audit, but they reassure you they are extremely eager to become CCSS certified so that they can ease their customers' minds and help repair the damage to their reputation.

The exchange operates in a way that it uses a browser-based wallet plugin communicating over web3.js libraries. Customers can grant access from the browser-based wallet plugin to the decentralized exchange through a web interface. Once the wallet plugin and exchange can talk to each other, customers are then free to make deposits, withdrawals, or perform trades between coins. This ensures that the exchange never has to manage a customer's private keys. In order to help pay for the exchange operating expenses, a small fee is held for every customer transaction. This fee is sent to one of 5 pre-defined "feeder" addresses, and then swept weekly into a single "main" exchange wallet. From the notes provided by the Security Engineer, it's determined that the exchange's original customer service agent generated the mnemonic seed for these wallets using a NIST SP 800-90A compliant Deterministic Random Bit Generator. The agent no longer works for the exchange and appears to have changed their contact information. The exchange still retains and uses the original seed used to generate the 5 "feeder" addresses, but due to previous compromises, they are not comfortable disclosing how and where the seed is stored.

Customer service for the exchange used to be handled internally, but now is handled by an email-only managed service. The service collects information from customers and uses it to make a support ticket. This ensures that the exchange can keep a low employee headcount, have a suitable level of customer support, and not have to manage an internal support staff. At no time in the support process do any support systems or agents have access to customer's private key or funds.

Due to the recent compromise, the exchange hired a hacker to penetration test their information systems. The hacker did exploit some outdated software that was immediately patched, and also identified a need for more thorough business processes and documentation. The exchange states to you that they have been working on this for the past 3 months, but you haven't seen any updated documentation during your audit discovery process. Repeated requests for the documentation result in the same answer: that it's currently in progress.

After the compromise, the exchange destroyed all previous laptops and servers that were in use. Brand new equipment was recently assigned to the small number of exchange employees. The exchange Security Engineer personally attests to setting up each machine while ensuring full-disk encryption was turned on, screensaver timeouts were configured, and anti-virus software was installed. From a security policy perspective, exchange employees are required to patch their systems and change their passwords for their devices every 30 days.