Exam Scenario A

You are auditing a custodial cryptocurrency exchange for CryptoCurrency Security Standard (CCSS) compliance. The exchange is a new business that has been operating for 2 years. As such, the exchange wishes to attain a Level 2 CCSS certification in order to show their customers that the exchange is serious about security and protecting their customers' funds.

As part of your audit, you interview the management and employees at the exchange in order to get a better idea of the exhcange's policies and procedures. Based on your interviews, you determine that the exchange has been operating with a "best practice" security mindset as much as possible, but certain gaps may exist due to the age of the company.

The exchange operates in a way that collects deposits from select customers, while allowing them to place market and limit orders. These deposits are placed into new addresses that are generated by the exchange website. Once approved, there is no limit to the amount of trading a customer can do. If a customer wishes to withdraw their funds, they must open a ticket under their exchange account with the Customer Support department who will then manually build, verify destination addresses and amounts, and broadcast the transaction. Exchange customers can view a real-time balance of their own account, or the entire exchange reserve, at any time.

When originally creating the business, the executive staff generated the seed for the Bitcoin wallet used in the daily operation of their business over pizza and beer at the home of the Chief Technology Officer (CTO). The keys were generated on an offline fully encrypted laptop that stored the CTO's personal cryptocurrency holdings. Since the CTO already had a copy of the Electrum Bitcoin wallet installed on the laptop, the executives used that software to create a new wallet file. The executives chose to use the wallet password feature inside the Electrum software to protect access to the wallet. Once the seed and wallet was created, the wallet file was moved to a USB drive for future use. Each executive then copied a backup of the seed phrase on to a piece of paper and placed it in a personally marked envelope. Each executive was instructed to store the envelope containing their copy of the backup inside their own personal safe. The CTO then powered down the laptop and stored it in a locked safe inside their home.

Since the exchange is a new business, their staff is made up of only a handful of employees. Each employee is known to each other, and in some cases have been friends for years. One of the employees with Information Security experience brought in an outside friend who was tasked with performing a penetration test on the systems in use. One of the things the friend identified was a need for logging, as the exchange software did not have this functionality.

Over the past few months the exchange worked to add audit logging for all user and administrator actions to their product.

While the exchange is still new, the staff has been working diligently to create documentation for company policies and procedures. Some of the policies include things like enforcement of full disk encryption, screensaver timeouts, key-compromise protocols, granting and revoking of key access, detailed data sanitization policies, harassment policies, onboarding and offboarding checklists for each role in the company, and an Information Security policy that the entire staff is periodically trained on. Recently, the company hired a Documentation Administrator whose job is to make sure all of the policies are kept current and up to date.