CRYPTOCURRENCY
SECURITY STANDARD

Exam Scenario D

A remote midwestern farming business in the United States has reached out to you to perform an audit so that they may pursue a level of CryptoCurrency Security Standard (CCSS) compliance and generate more traffic for their family business.

The family farm has traditionally operated within a standard banking system for the past three generations. Within the last few years, one of the teenage children in the family suggested the farm start accepting cryptocurrency payments for items that they sell through the local farmers market, payments from select resellers, and also directly from customers on the farm website.

The teenage daughter set the family up with a web portal allowing customers to pay using QR codes over TLS/SSL. The web portal contains a BIP32 xprv and the xpub and uses this to generate a new address and corresponding QR code for each transaction. The BIP32 private key was generated by the teenager using the bitcoind application on the farm's computer when setting up the web portal. At the time of the key generation, paper backup containing the BIP39 mnemonic seed words with a passphrase was created and stored in a non-transparent waterproof plastic bag sealed with security tape inside an old fireproof family safe in the loft of the barn.

The addresses that receive funds are swept each month, and the funds are converted into another cryptocurrency and automatically sent to a smart contract. The smart contract divides up the funds between all owners of the farm and distributes the funds to a static address for each family member. This distribution process takes place every 3 months. Family members are free to choose what they wish with funds after their distribution takes place.

As part of the farm's operational manual, a rough plan is outlined on what to do if disaster strikes or if the farm is hacked. The daughter has traditionally handled the responsibility of fixing the web portal and payment system as she was the one who created it, and the plan indicates to contact her when things stop working.

Up until recently, the daughter was the main point of contact for most parts of the payment system. Since leaving the farm to attend college overseas, the teenager's responsibilities have been transferred to the father in the family. While the father understands how the system works at a high level, his skills and knowledge are limited to what he can find on the Internet and web forum searches. The farm's operational manual was updated to list the father as the new point of contact for any disasters or compromises, but he ultimately does not feel comfortable or knowledgeable enough to handle this responsibility.

Since taking over the system, the father wishes to support more types of cryptocurrency coins and has identified a few things he wants to change including scheduling an external third party security review, generating new key material, and creating more backups of the seed material for disaster recovery purposes.