



CCSSI v9.0: Exam Scenario M

A mid-sized firm provides digital asset custody services for retail and institutional customers. It supports BTC and ETH deposits and withdrawals, treasury transfers between hot wallets and cold storage, and institutional accounts with configurable withdrawal rules. The firm operates a customer support portal and a service status page that posts uptime and incident updates. Leadership wants to align the custody platform with CCSS, but has not selected a target CCSS level. The firm is focusing first on withdrawals because customers notice withdrawal delays and failures immediately and this is where hot wallet signing happens. A major product launch is scheduled in 90 days, and changes cannot interrupt withdrawals for more than 30 minutes.

Withdrawals begin in a web/mobile application. Customers authenticate with username/password, and multi-factor authentication is available but not enforced for all users. Customer support can perform certain account recovery actions after verification. Requests flow through an API gateway that routes traffic to backend services, applies rate limiting on internet-facing endpoints, and logs requests. Logging and monitoring are centralized, but security logs, including authentication activity, signing requests, and IAM/HSM policy changes, are stored in the same cloud account as production systems. Alerting is consistent for uptime and error rates, but limited for suspicious withdrawal activity and unusual signing behavior. All personnel who can impact the security of key material generation, management, or usage, including engineers with IAM or HSM administrative access and staff involved in hot wallet signing operations, undergo documented operator screening before receiving access.

A Wallet Service maintains customer balances and an internal ledger. It builds withdrawal requests and applies withdrawal limits. The Wallet Service sends signing requests to a Signing Service. The Signing Service is a backend software component that uses a dedicated service account to authenticate to the cloud HSM and request transaction signatures. The hot wallet private keys remain in the cloud HSM as non-exportable keys; the Signing Service does not retrieve key material. The Signing Service validates request format, but it does not enforce the withdrawal limits applied in the Wallet Service before requesting signatures from the HSM.

A small group of senior engineers administer cloud Identity and Access Management (IAM) and cloud HSM access policies using single sign-on (SSO). Privileged access is standing rather than time-bound, and evidence for privileged changes is inconsistent across teams. The firm maintains runbooks and policies, but some documentation does not match current practice and diagrams are not consistently current.

Cold storage is used for treasury reserves and relies on an offline, in-person ceremony process, but procedures and evidence collection vary by team and are not consistently standardized.



Requests to grant or revoke access to IAM and HSM signing permissions are submitted and approved only through the company's approved ticketing system which enforces multi-factor authentication, and approvals are recorded. The firm also maintains a written key management roles and responsibilities document for hot wallet signing, HSM administration, and cold storage ceremonies, but the individuals assigned these responsibilities are not required to formally acknowledge their responsibilities in writing.

You are hired as the CCSS Implementer to define what's in scope for withdrawals, especially anything that can trigger signing or change signing access, perform a gap assessment against CCSS requirements, propose a target CCSS level, and deliver a prioritized implementation plan with phases, owners, and dependencies. You must also recommend the minimum documentation that will be kept current, including withdrawal flow diagrams, a key inventory and key lifecycle documentation, privileged access and change checklists, consistent records for cold ceremonies, and logging/monitoring review procedures, without turning the effort into a documentation project that no one maintains.

NOTE: This exam scenario is designed to test your ability to analyze and apply the CCSS from an implementer perspective based on the information provided. Please keep the following in mind:

- *Only consider the facts and 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 this scenario is to assess your ability to map given facts to CCSS requirements and identify what would be needed to meet a target level.*
- *Focus on implementer decisions and outputs, such as scoping, gap identification, prioritization, and recommending practical controls and documentation artifacts.*
- *For the purpose of this exam, focus only on what is explicitly presented in the scenario and what can be concluded from those facts.*