KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **CCSFP**

Title : Certified CSF Practitioner 2025 Exam

Version : DEMO

1.An organization has identified a number of components needed for an assessment. These components cover systems/applications for customers in the states of Massachusetts and Nevada.
Assuming management wants corresponding regulatory factors to be included in their assessment, which regulatory factors would apply? (Select all that apply)
A. State of Massachusetts Data Protection Act
B. CMS Minimum Security Requirements (High)
C. State of Nevada Security of Personal Information Requirements
D. Texas Health and Safety Code
E. Subject to De-ID Requirements
Answer: A, C
Explanation:
When performing HITRUST scoping, organizations must include regulatory factors relevant to their operational and geographic context. Since this entity operates in Massachusetts and Nevada, two state-specific privacy and security laws apply:
Massachusetts Data Protection Act (201 CMR 17.00): Requires businesses handling personal data of Massachusetts residents to maintain a written information security program (WISP), including encryption and monitoring controls.
Nevada Security of Personal Information Law (NRS 603A): Mandates encryption for personal information stored or transmitted electronically and requires reasonable security measures.
The CMS Minimum Security Requirements (High) (B) would apply only if the entity processes Medicare/Medicaid-related data. The Texas Health and Safety Code (D) applies only to Texas-based covered entities. Subject to De-ID Requirements (E) is a general data-handling condition, not a state-specific regulatory factor.
Therefore, only Massachusetts Data Protection Act and Nevada Security of Personal Information Requirements apply in this scenario.
Reference: HITRUST CSF Assurance Program – “Regulatory Factor Scoping”; CCSFP Study Guide – “State-Specific Regulatory Factors.”

2.The HITRUST QA reservation must be made by the External Assessor at least six months in advance of the submission date.
A. True
B. False
Answer: B
Explanation:
HITRUST requires External Assessors to reserve QA slots prior to submitting validated assessments. This ensures QA capacity is available and assessments are reviewed in a timely manner. However, the guidance does not specify a strict six-month minimum reservation period. Instead, HITRUST recommends assessors reserve QA slots well in advance of their submission target date, based on the anticipated complexity and workload. In practice, reservations may often be made months in advance, but there is no formal rule mandating six months. The flexibility allows assessors to adjust their schedules while ensuring HITRUST can properly plan QA resources. As such, the statement that reservations must always be made six months ahead is False.
Reference: HITRUST CSF Assurance Program Guide – “QA Reservation and Scheduling”; CCSFP Training – “Assessment Submission & QA.”

3.Firewalls with identical configurations can be grouped for testing as one component.
A. True
B. False
Answer: A
Explanation:
In HITRUST assessments, grouping is allowed when multiple primary components (like firewalls) are functionally identical in terms of configuration, management, and security controls. If all firewalls share the same rule sets, firmware, patching schedule, and are managed consistently, they can be grouped as one for testing purposes. This prevents repetitive validation work across systems that present no material differences in control design or operation. However, grouping requires justification and supporting documentation, showing that the systems are identical. If variations exist (e.g., differing rule sets or management practices), each firewall must be treated as a separate component. Grouping improves efficiency in large environments but must be applied cautiously to maintain the accuracy and integrity of testing results.
Reference: HITRUST CSF Assessment Methodology – “Component Identification & Grouping”; CCSFP Practitioner Training – “Scoping Components.”

4.The A1 Security Assessment requirements can only be added to the r2 assessment type.
A. True
B. False
Answer: B
Explanation:
The A1 Security Assessment factor is an optional module that introduces requirements for evaluating the security and governance of AI-based systems. These requirements are mapped into HITRUST CSF across domains like risk management, monitoring, and governance. Importantly, the A1 factor is not restricted solely to r2 assessments. While r2 provides the most comprehensive assurance model, A1 can also be added to other eligible assessment types such as i1 when the scope involves AI risks. The factor is treated like any other regulatory or organizational factor in MyCSF—its selection generates additional tailored requirement statements. Therefore, the claim that A1 can only be added to r2 is inaccurate. The correct understanding is that A1 can apply to multiple assessment types, depending on scoping decisions.
Reference: HITRUST CSF Extensions – A1 Security Assessment Factor; CCSFP Study Materials – “Emerging Risks & Add-On Factors.”

5.Gaps with required CAPS must have documented remediation plans within the assessment object before submission to HITRUST QA.
A. True
B. False
Answer: A
Explanation:
When a requirement statement or control reference fails to meet the HITRUST scoring threshold, a Corrective Action Plan (CAP) may be required. CAPs represent formal remediation commitments that must be documented in the assessment object before submission to QA. Each CAP must include details

such as the control deficiency, planned remediation steps, responsible parties, milestones, and expected completion dates. HITRUST QA will verify that all required CAPs are present before accepting the assessment for review. Without CAP documentation, the assessment submission is considered incomplete. This process ensures transparency and accountability and demonstrates to relying parties that the organization has a structured plan to close gaps. Therefore, the statement is True.
Reference: HITRUST Assurance Program Requirements – “CAP Documentation”; CCSFP Practitioner Guide – “CAPs and Submission Readiness.”