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 : **CIS-DF**

Title : Certified Implementation Specialist - Data Foundations (CMDB and CSDM)

Version : DEMO

1.A CMDB Administrator is implementing Vulnerability Response or Security Incident Response and needs to ensure customers have enough context to estimate risk and set task priorities.
Which Get Well Playbook from the CSDM Data Foundations Dashboard helps with this?
A. Locations without a Parent Location
B. Application Services with Business Application Relationships
C. Named Product Models without Product Owners
D. Percentage of Custom Status Values for CI Life Cycle Stages
Answer: B
Explanation:
In ServiceNow, Vulnerability Response and Security Incident Response rely heavily on business context to accurately assess risk, prioritize remediation tasks, and communicate impact to stakeholders. From a CSDM (Common Service Data Model) perspective, this context is primarily delivered through properly modeled relationships between Application Services and Business Applications.
The “Application Services with Business Application Relationships” Get Well Playbook directly addresses this requirement. In CSDM, Application Services represent the technical, deployable services that run in the environment, while Business Applications represent the logical applications that support business capabilities. When these two are correctly related, security teams can clearly understand which business processes, customers, and revenue streams are affected by a vulnerability or security incident.
Without this relationship, vulnerabilities may still be detected, but they lack meaningful prioritization. For example, a critical vulnerability on an application service supporting a revenue-generating or customer-facing business application should be addressed far more urgently than one tied to a low-impact internal tool. This relationship is what enables risk-based prioritization, rather than purely technical severity-based prioritization.
The other options do not fulfill this need. Location hierarchy issues (Option A) and CI lifecycle status consistency (Option D) relate more to CMDB hygiene and governance, not security context. Product ownership gaps (Option C) affect accountability but do not directly enable risk estimation during security response.
Therefore, Option B is the correct and CSDM-aligned Get Well Playbook for ensuring sufficient business context in Vulnerability Response and Security Incident Response workflows.

2.A customer’s CMDB is aligned to the CSDM Walk stage.
What benefit is provided by the CMDB?
A. Allows for additional stratification of technical teams’ support structure along the lines of OLAs and commitments
B. Improves the implementation velocity of APM Foundation for future business application rationalization
C. Enables impact assessments for incident, problem, and change on Business Services
Answer: C
Explanation:
In the CSDM Walk stage, an organization has moved beyond basic data hygiene (Crawl) and has established foundational service models, especially Business Services and their relationships to underlying technical components. One of the most important and immediate benefits of reaching this stage is the ability to perform reliable impact analysis across ITSM processes.
When Business Services are correctly defined and related to Application Services, applications, and

infrastructure CIs, the CMDB becomes a decision-support system rather than just a data repository. This enables impact assessments for Incident, Problem, and Change Management, which is exactly what Option C describes. For example, when an incident is logged against a CI, ServiceNow can automatically determine which Business Services are impacted and who the affected stakeholders are. Similarly, during Change Management, planners can assess downstream risk by identifying which business-facing services could be disrupted.
Option A is more aligned with advanced operational governance and support model optimization, which typically appears later as organizations mature toward the Run stage.
Option B relates to Application Portfolio Management (APM) acceleration, which benefits more from accurate application ownership and lifecycle data rather than core Walk-stage service modeling.
Therefore, the correct and CSDM-aligned benefit at the Walk stage is enabling impact assessments for incident, problem, and change on Business Services, making Option C the verified answer.

3.A CMDB Administrator needs to import external data into the CMDB. To reduce the risk of creating duplicates and prevent updates from unauthorized sources, it must be ensured that the Identification and Reconciliation Engine (IRE) is not bypassed.
What is the recommended method to import data into the CMDB utilizing the Identification and Reconciliation API?
A. IntegrationHub ETL
B. Table API (REST API or SOAP API)
C. Import Sets and Transform Maps
Answer: A
Explanation:
In ServiceNow, protecting CMDB data quality during ingestion is a core Data Foundations principle. The Identification and Reconciliation Engine (IRE) is designed to ensure that CI records are uniquely identified, merged correctly, and protected from unauthorized overwrites. Any ingestion method that bypasses IRE introduces a high risk of duplicates and data corruption.
IntegrationHub ETL is the recommended method because it is natively designed to work with the Identification and Reconciliation API. When properly configured, IntegrationHub ETL ensures that incoming data is processed through IRE, applying identification rules, reconciliation rules, and source precedence. This allows multiple data sources to coexist safely while maintaining CMDB integrity.
Option B (Table API) is explicitly discouraged for CMDB ingestion because it writes directly to CMDB tables and bypasses IRE entirely, making it one of the most common causes of duplicate and conflicting CI records. While REST and SOAP APIs are powerful, they are not safe for CMDB ingestion unless they explicitly invoke the IRE API, which most generic table integrations do not.
Option C (Import Sets and Transform Maps) can be configured to call IRE, but this requires additional scripting and strict governance. Because of this complexity and higher risk of misconfiguration, it is not the recommended approach when safer, purpose-built options exist.
Therefore, IntegrationHub ETL is the verified and best-practice answer, making Option A correct.

4.(Choose 2 options)
A CMDB Administrator has built a number of Technology Management Service Offerings (Technical Service Offerings) based on Dynamic CI Groups to better maintain group alignment for the member CIs.
Which groups are synced to CIs from the offering that has a relationship to a Dynamic CI Group?

A. Approval Group
B. Managed by Group
C. Owned by Group
D. Support Group
Answer: BD
Explanation:
In ServiceNow, Dynamic CI Groups are a core Data Foundations capability used to automatically manage CI membership based on rules rather than manual maintenance. When Technology Management Service Offerings (Technical Service Offerings) are related to Dynamic CI Groups, ServiceNow uses those relationships to synchronize operational support attributes to the member CIs. The two CI attributes that are intentionally designed to sync in this model are the Managed by Group and the Support Group. These groups directly influence operational ownership and support routing, which is why they are automatically aligned when Dynamic CI Groups are used. This ensures that incidents, changes, problems, and operational tasks are routed consistently as CI membership changes over time.
The Support Group defines who provides day-to-day operational support and is critical for Incident and Request Management workflows. The Managed by Group represents the team responsible for the technical lifecycle and operational health of the CI. Synchronizing these attributes eliminates manual updates and reduces misrouted tickets, which is a key goal of Configuration Management maturity.
The Approval Group (Option A) is not synced because approvals are process-driven and often context-specific rather than CI-driven. Similarly, the Owned by Group (Option C) represents accountability or financial ownership, which is intentionally decoupled from dynamic operational grouping to avoid unintended governance changes.
Therefore, the correct answers are B (Managed by Group) and D (Support Group).

5.Which is a purpose or requirement of CMDB Data Manager in ServiceNow?
A. Encrypts archived records for enhanced security
B. Automates the enforcement of relationship rules between CIs in the CMDB
C. Automates the archival and deletion of records based on retention policies
Answer: C
Explanation:
The CMDB Data Manager capability in ServiceNow is designed to support CMDB governance, specifically around data lifecycle management. Its primary purpose is to ensure that CI records are retained, archived, and deleted in accordance with defined retention policies, regulatory requirements, and organizational data governance standards.
As CMDBs mature, they naturally accumulate obsolete, retired, or decommissioned CIs. If these records are not properly managed, they negatively impact CMDB health, reporting accuracy, discovery reconciliation, and performance. CMDB Data Manager addresses this by automating the archival and deletion of records once lifecycle conditions and retention thresholds are met.
Option A is incorrect because encryption of archived records is handled by platform-level security and data protection features, not CMDB Data Manager.
Option B is also incorrect because relationship rule enforcement is managed through CSDM guidance, CMDB relationship rules, and identification/reconciliation logic—not by CMDB Data Manager.
By automating retention-based archival and cleanup, CMDB Data Manager helps organizations maintain

a lean, compliant, and high-quality CMDB, which directly supports CMDB Health metrics such as correctness and compliance.
Therefore, the correct and verified answer is Option C.