Number: CTA
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: CTA

Exam Name: ServiceNow Certified Technical Architect

Exam A

QUESTION 1
What are the primary capabilities of Service Mapping in ServiceNow?
Choose 2 answers

A. Create a service-centric Configuration Management Database (CMDB)
B. Enhance cybersecurity measures across systems
C. Automate routine IT infrastructure updates
D. Oversee software licensing for various platforms
E. Establish links between IT infrastructure components and application services

Correct Answer: A, E
Section:
Explanation:
Service Mapping in ServiceNow has two primary capabilities:
A . Create a service-centric Configuration Management Database (CMDB): Service Mapping helps shift the focus of the CMDB from individual components to a service-centric view. It achieves this by mapping the relationships between infrastructure components and the services they support, providing a clear understanding of how IT supports business services.
E . Establish links between IT infrastructure components and application services: This is the core function of Service Mapping. It automatically discovers and maps the dependencies between applications, infrastructure (servers, databases, network devices), and the services they deliver. This creates a visual representation of the IT landscape and how it supports business services.
Why not the other options?
B: While Service Mapping can indirectly contribute to cybersecurity by providing visibility into the IT environment, enhancing cybersecurity measures is not its primary function.
C: Automating routine IT infrastructure updates is typically handled by other ServiceNow capabilities like Orchestration, not Service Mapping.
D: Software licensing management is usually handled by Software Asset Management tools, not Service Mapping.

QUESTION 2
What does a ServiceNow governance framework typically define?
Choose 3 answers

A. How decisions are made
B. What decisions need to be made
C. Who is involved in decision-making
D. Recurring schedules for governance meetings
E. How work gets done on the platform

Correct Answer: A, B, C
Section:
Explanation:
A ServiceNow governance framework provides structure and guidance for managing the platform and its applications. It typically defines:
A . How decisions are made: The framework outlines the processes for making decisions related to the platform, such as changes to configurations, new application development, and platform upgrades. This might include approval processes, escalation procedures, and communication protocols.
B . What decisions need to be made: The framework identifies the types of decisions that require governance oversight. This might include decisions about platform strategy, architecture, security, data management, and integration with other systems.
C . Who is involved in decision-making: The framework establishes roles and responsibilities for different stakeholders in the governance process. This might include defining a governance board, steering committees, and individual roles with specific decision-making authority.

Why not the other options?
D: While recurring schedules for governance meetings are important, they are not a defining element of the governance framework itself. The framework focuses on the overall structure and processes for decision-making.
E: How work gets done on the platform is more related to process definitions and workflows within specific applications, not the overarching governance framework.

QUESTION 3
A new project request requires quick implementation but involves portfolio realignment. As an IT leader, who should you consult to prioritize this demand?

A. Demand Board
B. Executive Steering Board
C. Program Steering Committee
D. Technical Governance Board

Correct Answer: B
Section:
Explanation:
In this scenario, the Executive Steering Board is the most appropriate group to consult. Here's why:
Portfolio Realignment: This implies significant changes to the overall IT portfolio, which falls under the purview of the Executive Steering Board. They have the authority to make strategic decisions about the IT portfolio and prioritize initiatives based on business goals and overall impact.
Why not the other options?
A . Demand Board: The Demand Board typically focuses on evaluating and prioritizing individual demands or requests, but they may not have the authority to make decisions about portfolio realignment.
C . Program Steering Committee: This committee focuses on the governance and oversight of specific programs, not on overall portfolio strategy.
D . Technical Governance Board: This board focuses on technical standards, architecture, and security, not on strategic portfolio decisions.

QUESTION 4
Under technical governance policies, what does environmental management in ServiceNow primarily define?

A. Instance structure
B. Data ownership
C. User access policies
D. Application customization

Correct Answer: A
Section:
Explanation:
In the context of ServiceNow technical governance, environmental management primarily focuses on defining the instance structure. This includes:
Instance Segmentation: Determining how many instances are needed (e.g., separate instances for development, test, and production) and how they relate to each other.
Instance Upgrades: Establishing policies and procedures for managing instance upgrades, including scheduling, testing, and communication.
Instance Maintenance: Defining guidelines for ongoing maintenance activities, such as patching, backups, and performance monitoring.
Why not the other options?
B . Data ownership: Data ownership is typically addressed within data governance policies, not specifically environmental management.
C . User access policies: User access policies are part of security governance and are handled through roles, permissions, and access control lists.
D . Application customization: Application customization is governed by development and configuration standards, not directly by environmental management.

QUESTION 5
A company is preparing for a ServiceNow instance upgrade. Which tool shortens the time to validate critical processes post-upgrade?

A. Test Management 2.0
B. Automated Testing Framework (ATF)

C. Manual testing scripts
D. System health dashboard

Correct Answer: B
Section:
Explanation:
The Automated Testing Framework (ATF) is the best tool for quickly validating critical processes after a ServiceNow instance upgrade. Here's why:
Automated Execution: ATF allows you to create automated tests that can be run quickly and repeatedly after the upgrade. This significantly reduces the time required for testing compared to manual methods.
Comprehensive Coverage: You can create automated tests for various processes, workflows, UI actions, and business rules, ensuring comprehensive validation of critical functionality.
Regression Testing: ATF is particularly valuable for regression testing, ensuring that the upgrade hasn't introduced any unexpected issues or broken existing functionality.
Why not the other options?
A . Test Management 2.0: While Test Management 2.0 provides a framework for managing tests, it doesn't inherently shorten the testing time itself. It can be used with ATF to organize and track automated tests.
C . Manual testing scripts: Manual testing is time-consuming and prone to errors, especially for repetitive tasks involved in upgrade validation.
D . System health dashboard: This dashboard provides an overview of system performance and health, but it doesn't directly validate specific processes or workflows.

QUESTION 6
What is the primary purpose of the Test Management 2.0 application in ServiceNow?

A. To streamline manual testing processes
B. To generate test cases automatically
C. To automate software testing processes
D. To replace human testers with AI

Correct Answer: A
Section:
Explanation:
The primary purpose of Test Management 2.0 is to streamline manual testing processes. It provides a structured framework for:
Planning and Designing Tests: Creating test plans, test cases, and test suites.
Executing Tests: Tracking test execution and recording results.
Managing Defects: Logging and tracking defects found during testing.
Reporting: Generating reports on test coverage, progress, and results.
Why not the other options?
B . To generate test cases automatically: While Test Management 2.0 can help with test case design, it doesn't automatically generate them.
C . To automate software testing processes: This is the role of the Automated Testing Framework (ATF). Test Management 2.0 can be used alongside ATF to manage automated tests.
D . To replace human testers with AI: While AI can assist with testing, Test Management 2.0 is primarily designed to support human testers, not replace them.

QUESTION 7
What type of testing is characterized by an unplanned approach where the tester's understanding and insight are the most important factors?

A. Usability testing
B. Performance testing
C. Ad hoc testing
D. Load testing

Correct Answer: C
Section:
Explanation:
Ad hoc testing is characterized by an unplanned, informal approach where testers rely on their knowledge and intuition to explore the software and identify potential issues.

Key characteristics of ad hoc testing:
No predefined test cases: Testers don't follow specific scripts or steps.
Exploratory in nature: Testers freely explore the software, trying different actions and inputs.
Relies on tester experience: The effectiveness of ad hoc testing depends on the tester's understanding of the software and their ability to identify potential problem areas.
Why not the other options?
A . Usability testing: Focuses on user experience and follows a structured approach.
B . Performance testing: Evaluates system performance under different conditions (e.g., load, stress).
D . Load testing: A type of performance testing that simulates heavy user load.

QUESTION 8
What is the primary purpose of having a go-live plan?

A. To facilitate a seamless and smooth transition process.
B. To record root causes for problems arising out of the transition.
C. To establish a backup system for data recovery.
D. To conduct a comprehensive review of all project documents.

Correct Answer: A
Section:
Explanation:
The primary purpose of a go-live plan is to facilitate a seamless and smooth transition process when deploying new software or changes to a production environment. It acts as a roadmap for the go-live event, outlining the steps involved, roles and responsibilities, and timelines.
A go-live plan typically includes:
Pre-Go-Live Activities: Data migration, system checks, communication to users.
Go-Live Activities: Deployment steps, rollback procedures, monitoring.
Post-Go-Live Activities: Support procedures, user training, issue resolution.
Why not the other options?
B . To record root causes for problems arising out of the transition: While problem resolution is important, it's not the primary purpose of the go-live plan.
C . To establish a backup system for data recovery: Backups are essential, but they are a separate consideration from the go-live plan.
D . To conduct a comprehensive review of all project documents: This review should happen earlier in the project lifecycle.

QUESTION 9
Why is IP address access control considered part of the network layer despite being implemented in the application layer?

A. It performs data tokenization and substitution for security.
B. It uses encryption to protect data at rest in the ServiceNow instance.
C. It restricts access to the instance based on IP address ranges.
D. It manages user authentication to the ServiceNow platform.

Correct Answer: C
Section:
Explanation:
IP address access control is considered part of the network layer because it restricts access to the instance based on IP address ranges.
Here's why:
Network Layer Functionality: IP address filtering operates at the network level by controlling which IP addresses are allowed to connect to the ServiceNow instance. This is similar to firewall rules that control network traffic.
Application Layer Implementation: While the filtering might be implemented within the ServiceNow application (application layer), the underlying functionality is related to network access control.
Why not the other options?
A . It performs data tokenization and substitution for security: This is a data security technique, not related to network layer access control.
B . It uses encryption to protect data at rest in the ServiceNow instance: This is a data security measure, not network access control.

D . It manages user authentication to the ServiceNow platform: Authentication is a separate security layer (usually application layer) that verifies user identities.

QUESTION 10
What components constitute the application layer security within ServiceNow?
Choose 3 answers

A. Multi-Factor Authentication (MFA)
B. Platform Encryption (PE)
C. Access Control Lists (ACLs)
D. Full Disk Encryption (FDE)
E. IP address access control

Correct Answer: A, C, E
Section:
Explanation:
Application layer security in ServiceNow focuses on protecting data and functionality within the ServiceNow application itself. The following components contribute to this:
A . Multi-Factor Authentication (MFA): MFA adds an extra layer of security by requiring users to provide multiple forms of authentication (e.g., password, security token, biometric verification) to access the application.
C . Access Control Lists (ACLs): ACLs define which users or roles have permission to access, modify, or delete specific data and functionality within the application.
E . IP address access control: While technically a network layer control, IP address access control is often implemented and managed within the ServiceNow application. It restricts access to the instance based on IP address ranges.
Why not the other options?
B . Platform Encryption (PE): This is a broader encryption solution that protects data at rest across the platform, not specifically at the application layer.
D . Full Disk Encryption (FDE): This encrypts the entire hard drive of the server where the ServiceNow instance is hosted, providing protection at the infrastructure level, not the application layer.

QUESTION 11
What does the ServiceNow Security Center's daily compliance score indicate in ServiceNow?

A. The number of security incidents created in the last 24 hours.
B. The number of phishing emails resolved in the last 24 hours.
C. The security compliance percentage of the ServiceNow instance.
D. Percentage of vulnerabilities remediated in the last 24 hours.

Correct Answer: C
Section:
Explanation:
The ServiceNow Security Center's daily compliance score represents the security compliance percentage of the ServiceNow instance. It provides an overall measure of how well your instance adheres to defined security policies and best practices.
The score is calculated based on various factors, including:
Vulnerability Management: The number of identified vulnerabilities and their severity.
Configuration Compliance: How well the instance configuration aligns with security standards.
User Access Controls: The effectiveness of user access management and authentication.
Security Incident Management: The handling and resolution of security incidents.

QUESTION 12
A system administrator needs to ensure that sensitive customer data in fields is only accessible to specific roles within a ServiceNow instance. Which feature should be utilized?

A. PI1 Encryption
B. Column Level Encryption (CLE)

C. Cloud Encryption
D. Full Disk Encryption (FDE)

Correct Answer: B
Section:
Explanation:
To control access to sensitive data at the field level, the system administrator should use Column Level Encryption (CLE).
Here's how CLE works:
Field-Level Encryption: CLE allows you to encrypt specific fields within a table, ensuring that only authorized users with the necessary decryption keys can access the data.
Granular Control: You can define different encryption keys for different fields or groups of fields, providing fine-grained control over data access.
Role-Based Access: You can grant access to decryption keys based on user roles, ensuring that only authorized personnel can view sensitive information.
Why not the other options?
A . PI1 Encryption: This is not a standard ServiceNow encryption feature.
C . Cloud Encryption: This is a broader term for encryption solutions provided by cloud providers, not a specific ServiceNow feature.
D . Full Disk Encryption (FDE): This encrypts the entire hard drive, not individual fields within the application.

QUESTION 13
Starting with the Washington DC release, what will replace Database Encryption for data at rest in ServiceNow?

A. Column Level Encryption (CLE)
B. Cloud Encryption
C. Full Disk Encryption (FDE)
D. IP Address Access control (IPAC)

Correct Answer: B
Section:
Explanation:
Starting with the Washington DC release, ServiceNow is transitioning from Database Encryption to Cloud Encryption for protecting data at rest.
Cloud Encryption: This leverages the encryption capabilities of the underlying cloud infrastructure (e.g., AWS, Azure) to provide a more robust and scalable encryption solution.
Enhanced Security: Cloud Encryption offers improved key management and security features compared to the previous Database Encryption.
Simplified Management: It reduces the administrative overhead associated with managing encryption keys.

QUESTION 14
A system administrator, Priya, notices that certain Configuration Items (CIs) in the CMDB have not populated the required and recommended fields, impacting data integrity. Which KPI should Priya review to diagnose this issue?

A. Compliance
B. Correctness
C. Completeness
D. Relationships

Correct Answer: C
Section:
Explanation:
The KPI that directly relates to the issue of missing required and recommended fields is Completeness.
Completeness: This KPI measures the extent to which CI records have all the necessary information filled in. Missing required or recommended fields indicate a lack of completeness in the CMDB data.
Why not the other options?
Compliance: Compliance focuses on whether CIs meet defined standards and policies, not necessarily on the completeness of their data.

Correctness: Correctness relates to the accuracy of the data in the CMDB, not whether all required fields are populated.
Relationships: Relationships measure the connections between CIs, not the completeness of individual CI records.

QUESTION 15
What action does the Identification and Reconciliation module perform to reduce duplicates in the CMDB?

A. Merges duplicate records automatically
B. Uses identification rules to uniquely identify CIs
C. Validates data sources to ensure accuracy
D. Assigns unique identifiers to each CI

Correct Answer: B
Section:
Explanation:
The Identification and Reconciliation (I&R) module uses identification rules to uniquely identify CIs. These rules help the system determine if a CI discovered or imported from a data source already exists in the CMDB or if it's a new CI.
Here's how it works:
Identification Rules: These rules define criteria for matching CIs based on their attributes (e.g., serial number, MAC address, hostname).
Matching and Reconciliation: When new data comes in, the I&R engine applies the rules to find potential matches. If a match is found, the system can either update the existing CI with new information or flag it as a potential duplicate for review.
Why not the other options?
A: While the I&R engine can facilitate merging duplicates, it doesn't automatically merge them without human review and approval.
C: Data source validation is important, but it's not the primary function of the I&R engine in duplicate reduction.
D: Assigning unique identifiers is a function of the CMDB itself, not specifically the I&R engine.

QUESTION 16
Which methods can be used to populate the CMDB with data from third-party sources? Choose 2 answers

A. Identification and Reconciliation Engine (IRE)
B. Discovery
C. IntegrationHub ETL
D. Service Graph Connectors
E. Service Mapping

Correct Answer: C, D
Section:
Explanation:
The two primary methods for populating the CMDB with data from third-party sources are:
C . IntegrationHub ETL: IntegrationHub ETL (Extract, Transform, Load) allows you to connect to various data sources, extract data, transform it to match the CMDB structure, and load it into the CMDB. This is a very flexible and powerful tool for integrating with a wide range of third-party systems.
D . Service Graph Connectors: Service Graph Connectors are pre-built integrations that connect ServiceNow to specific third-party applications and services. They provide a streamlined way to import data from these sources into the CMDB.
Why not the other options?
A: The I&R engine primarily focuses on identifying and reconciling CIs, not on the initial population of data from external sources.
B: Discovery is used to automatically discover and populate information about devices and applications within your own network, not primarily from third-party sources.
E: Service Mapping focuses on discovering and mapping the relationships between applications and infrastructure components, not on importing data from external sources.

QUESTION 17

Which encryption solution would ensure that customer credit card numbers were encrypted before being stored in the cloud and would allow for easy administration of encryption keys?

A. Edge Encryption
B. Server-side Encryption
C. Client-side Encryption
D. Database Encryption

Correct Answer: C
Section:
Explanation:
Client-side Encryption is the best solution to encrypt customer credit card numbers before they are stored in the cloud and provide easy key management. Here's why:
Encryption Before Storage: Data is encrypted on the client-side (e.g., user's browser or device) before being sent to the cloud, ensuring that even if the cloud storage is compromised, the sensitive data remains protected.
Key Management: The encryption keys are managed by the client or a trusted key management system, providing greater control and flexibility.
Reduced Risk: Client-side encryption minimizes the risk of sensitive data being exposed in the cloud environment.
Why not the other options?
A . Edge Encryption: This is a broader term that can refer to various encryption techniques applied at the edge of the network.
B . Server-side Encryption: Data is encrypted on the server-side, which means the cloud provider has access to the encryption keys.
D . Database Encryption: This encrypts the entire database, but it doesn't provide the same level of control and key management as client-side encryption.

QUESTION 18
What approach reduces complexity and maintenance overhead when assigning data ownership?

A. Assigning data ownership by location
B. Assigning data ownership by role
C. Assigning data ownership by attribute
D. Assigning data ownership by entity

Correct Answer: B
Section:
Explanation:
Assigning data ownership by role is the most effective way to reduce complexity and maintenance overhead. Here's why:
Clear Responsibility: Roles are associated with specific responsibilities and functions within an organization. Assigning data ownership to a role ensures that someone is clearly accountable for the quality and accuracy of that data.
Reduced Overhead: When people change positions or leave the organization, the data ownership remains with the role, not the individual. This reduces the need to constantly update ownership assignments.
Consistency: Role-based ownership promotes consistency in data management practices and ensures that data is handled according to defined standards.
Why not the other options?
A . Assigning data ownership by location: This can create confusion and inconsistencies, especially in organizations with multiple locations or remote teams.
C . Assigning data ownership by attribute: This can be overly granular and difficult to manage, especially for large datasets.
D . Assigning data ownership by entity: This can lead to unclear ownership and potential conflicts if multiple entities are involved with the same data.

QUESTION 19
When should security be set up in the ServiceNow application build process?

A. Only when issues are encountered during operations
B. After configuring all the application workspaces
C. After configuring all required integrations
D. Before configuring interfaces or business logic

Correct Answer: D
Section:
Explanation:
Security should be established before configuring interfaces or business logic in the ServiceNow application build process. This is known as 'security by design.'
Here's why:
Prevent Security Gaps: Building security into the application from the start helps prevent vulnerabilities and security gaps that can be exploited later.
Reduce Rework: Addressing security early avoids costly rework later if security issues are discovered after development is complete.
Enforce Best Practices: Starting with security ensures that security best practices are followed throughout the development process.
Why not the other options?
A . Only when issues are encountered during operations: This is a reactive approach that can lead to significant security risks.
B . After configuring all the application workspaces: Security should be integrated throughout the application, not just in specific workspaces.
C . After configuring all required integrations: Security should be considered before and during integration to ensure secure data exchange.

QUESTION 20
Which data types are considered part of Master/Core Data in ServiceNow?
Choose 3 answers

A. Approval Policies
B. Transaction logs
C. CMDB data
D. Service model data
E. User information

Correct Answer: A, C, E
Section:
Explanation:
Master/Core data in ServiceNow refers to the foundational data that is essential for the platform's operation and various applications. This includes:
A . Approval Policies: These define the rules and workflows for approvals within the platform, impacting various processes.
C . CMDB data: The Configuration Management Database (CMDB) contains critical information about IT assets, services, and their relationships.
E . User information: Data about users, their roles, and their permissions is crucial for access control and security.
Why not the other options?
B . Transaction logs: These are operational data that record system activities, not core master data.
D . Service model data: While important, service model data is typically built upon the foundation of master data like the CMDB and user information.

QUESTION 21
Which strategy is recommended for effective communication during the go-live phase?

A. Focus communications only on immediate supervisors.
B. Provide minimal updates to avoid overloading the team.
C. Postpone any form of communication until all issues are resolved.
D. Describe released functionality and provide knowledge base articles.

Correct Answer: D
Section:
Explanation:
Effective communication during a go-live is crucial for keeping stakeholders informed and managing expectations. The best strategy is to describe released functionality and provide knowledge base articles. Here's why:
Clarity and Transparency: Clearly communicate what new features or changes are being released, so users understand what to expect.
Knowledge Base Articles: Provide detailed documentation and knowledge base articles to help users learn about the new functionality and how to use it.

Proactive Communication: Don't wait for issues to arise before communicating. Keep users informed about the progress of the go-live and any potential impacts.
Targeted Communication: Tailor communication to different audiences (e.g., end-users, IT staff, management).
Why not the other options?
A . Focus communications only on immediate supervisors: This limits information flow and can lead to confusion and frustration among other stakeholders.
B . Provide minimal updates to avoid overloading the team: Under-communication can create anxiety and uncertainty. It's better to provide regular, concise updates.
C . Postpone any form of communication until all issues are resolved: This is unrealistic and can damage trust. Communicate openly about challenges and progress towards resolution.

QUESTION 22
What should be included in the go-live planning to handle and manage potential risks?

A. A list of key performance metrics to track the performance.
B. A back-out plan and mitigation plan for unforeseen circumstances.
C. A detailed communication plan for all stakeholders.
D. A schedule for user training and support sessions.

Correct Answer: B
Section:
Explanation:
To effectively manage risks during a go-live, it's essential to have a back-out plan and mitigation plan for unforeseen circumstances. This includes:
Back-out Plan: A detailed procedure for reverting to the previous system or version if the go-live encounters critical issues.
Mitigation Plans: Prepared responses for anticipated risks (e.g., data migration errors, performance issues, user resistance). These plans outline steps to address these risks if they occur.
Risk Assessment: A thorough risk assessment should be conducted before the go-live to identify potential risks and their likelihood.
Why not the other options?
A . A list of key performance metrics to track the performance: While performance monitoring is important, it's not the primary element for managing risks.
C . A detailed communication plan for all stakeholders: Communication is crucial, but it's a separate component of the go-live plan.
D . A schedule for user training and support sessions: User training and support are important but not directly related to risk management.

QUESTION 23
What is the primary purpose of security threat modeling?

A. To identify potential threats and develop mitigations.
B. To manage the encryption key management process.
C. To backup, restore and recover critical customer data.
D. To configure trusted IP address ranges in the system.

Correct Answer: A
Section:
Explanation:
The primary purpose of security threat modeling is to identify potential threats and develop mitigations. It involves:
Analyzing the System: Understanding the architecture, components, and data flows of the system.
Identifying Threats: Identifying potential security threats and vulnerabilities.
Assessing Risk: Evaluating the likelihood and impact of each threat.
Developing Mitigations: Designing and implementing security controls to reduce or eliminate the identified risks.
Why not the other options?
B . To manage the encryption key management process: This is a specific security activity, not the primary purpose of threat modeling.
C . To backup, restore and recover critical customer data: This is related to data protection and disaster recovery, not threat modeling.
D . To configure trusted IP address ranges in the system: This is a specific security control, not the overarching goal of threat modeling.