Servicenow

(CIS-RC)

Certified Implementation Specialist - Risk and Compliance

Total: **187 Questions**

Link:

Question: 1

Which of the following tables exist within the GRC: Profiles application scope? (Choose three.)

A.Document
B.Policy
C.Risk
D.Content
E.Indicator

Answer: ADE

Explanation:

The correct answer identifies tables existing within the ServiceNow GRC: Profiles application scope, crucial for managing organizational profiles and related elements. Here's a breakdown of why options A, D, and E are correct, and why B and C are incorrect:

A. Document: The Document table (often named something like sn_compliance_document or similar depending on the exact implementation) is a core element of the Profiles application. Organizations need to store and manage documents related to their profiles, whether they're regulatory filings, standard operating procedures, or other supporting materials. This aligns with the cloud computing concept of data management, where structured storage and organization of documents within a cloud-based application are key. The Profile type configuration will often relate to what documents should be kept.

D. Content: The Content table (or sn_grc_content or similar) isn't a direct profile-related table, but is connected to the policy and compliance functions and is available within the GRC application scope. Content is related to the storage of policy statements that are required for Profile compliance.

E. Indicator: In the GRC: Profiles context, Indicators allow organizations to track key performance indicators (KPIs) or key risk indicators (KRIs) that are associated with their profiles. This supports monitoring and reporting, crucial aspects of compliance and risk management. It aligns with the cloud computing concept of analytics and reporting, where GRC applications provide tools to visualize and analyze data related to risk and compliance.

B. Policy: While policies are crucial in GRC, the Policy table (or sn_compliance_policy typically) resides more directly within the broader GRC: Policy and Compliance application scope, not solely the Profiles application. The relationship is that profiles may be subject to specific policies.

C. Risk: The Risk table (often sn_risk_risk) also falls under the GRC: Risk Management application scope. While organizational profiles are exposed to risks, the Risks are not directly stored against the Profiles. The Profiles might be used to determine which risks are relevant to the profile.

In summary, the Document, Content and Indicator tables are directly relevant for managing profiles within the GRC: Profiles application scope, facilitating effective profile maintenance, compliance, and risk monitoring. Policies and Risks are related, but not directly stored against Profiles.

Question: 2

What are some characteristics of the ServiceNow Store? (Choose four.)

A.Some applications are certified by ServiceNow
B.All applications are certified by ServiceNow

C.Applications may be developed by ServiceNow Technology Partners
D.It houses both paid and free applications and integrations
E.Applications are built om the ServiceNow platform
F.Applications are certified by other developers

Answer: BCDE

Explanation:

The provided answer, BCDE, correctly identifies characteristics of the ServiceNow Store. Let's break down why:

B. All applications are certified by ServiceNow (Incorrect): This statement is incorrect. While ServiceNow certifies many apps to ensure quality and security, not all apps are necessarily certified. Some might be community-developed or earlier versions awaiting certification.

C. Applications may be developed by ServiceNow Technology Partners (Correct): The ServiceNow ecosystem thrives on collaboration. Technology Partners are key contributors, developing applications that extend the platform's functionality. This aligns with the platform-as-a-service (PaaS) model, where third-party developers can build on the core platform.

D. It houses both paid and free applications and integrations (Correct): The ServiceNow Store offers a variety of apps and integrations, some available for free and others requiring a purchase. This is a typical marketplace model, providing options to suit different needs and budgets.

E. Applications are built on the ServiceNow platform (Correct): Applications in the ServiceNow Store leverage the platform's underlying infrastructure, including its workflow engine, data model, and UI framework. This ensures seamless integration and consistent user experience. This is fundamental to ServiceNow's PaaS offering.

In conclusion, the ServiceNow Store is a marketplace built on the ServiceNow platform, offering a range of applications and integrations, developed by both ServiceNow and its Technology Partners, and available in both paid and free options.

Supporting Resources:

ServiceNow Store:https://store.servicenow.com/ (This link provides direct access to the ServiceNow Store, allowing you to explore available applications and integrations.)
ServiceNow Technology Partner Program: Search for "ServiceNow Partner Program" on the official ServiceNow website. (Provides details on the program that enables partners to develop and offer solutions in the store)

Question: 3

Which role is not part of ServiceNow GRC?

A.Risk User
B.Risk Developer
C.Risk Manager
D.Risk Reader

Answer: B

Explanation:

The correct answer is B. Risk Developer is **not** a standard, out-of-the-box role in ServiceNow GRC (Governance, Risk, and Compliance). While developers are crucial for customizing and extending the ServiceNow platform, including GRC applications, there isn't a specific dedicated "Risk Developer" role that directly grants permissions within the GRC module itself. Instead, developers leverage roles like admin or potentially custom roles granted specific access to GRC tables and functionalities.

Risk User, Risk Manager, and Risk Reader are all standard roles within ServiceNow GRC.

Risk User: Can create and manage risk events, tasks, and assessments. They are involved in the day-to-day operations of risk management.
Risk Manager: Oversees the entire risk management program, defines policies, assigns tasks, and reviews risk data. They have broader administrative privileges within the Risk application.
Risk Reader: Primarily has read-only access to risk information, allowing them to view reports, dashboards, and other relevant data without the ability to modify anything. This role is suitable for stakeholders who need visibility into the organization's risk posture.

The need for development-related activities in GRC environments is recognized; however, they are typically handled by developers who are assigned existing roles that give them general admin capabilities on the instance or are provided granular permissions through custom roles created by the customer. These custom roles are then tailored based on the precise development tasks being executed within the GRC environment, rather than through a single "Risk Developer" role included within the GRC module itself. These developers would be expected to adhere to DevOps principles and follow standard software development processes when working on any customizations for the GRC application to keep compliance integrity.

Further Research:

ServiceNow GRC Documentation: Check the official ServiceNow documentation for the specific version of GRC you're interested in. It will list the available roles and their associated permissions. [Search "ServiceNow GRC roles" in the ServiceNow product documentation portal]
ServiceNow Community Forums: Review ServiceNow community discussions to see how organizations handle development-related tasks within their GRC environments. [Search "ServiceNow GRC Development" on the ServiceNow Community site]

Question: 4

Which of the following statements is true of a Risk Response task?

A.Only one Risk Response task can be related to a Risk at a time
B.Only users with the risk_manager role or higher can be assigned to a Risk Response task
C.The risk admin role is required to assign the Risk Response task
D.The Risk Response task is automatically progressed through the states using a workflow

Answer: D

Explanation:

The correct answer is D: "The Risk Response task is automatically progressed through the states using a workflow."

Here's why: Risk Response tasks in ServiceNow's Risk Management module are designed to be automated and guided. A workflow drives the task's progression through different states (e.g., Open, Work in Progress, Closed). This automation ensures consistency and efficiency in handling risk responses. The workflow defines the sequence of actions, approvals, and notifications required to manage the risk response effectively.

Option A is incorrect because multiple Risk Response tasks can be related to a single Risk, as different responses may be required to mitigate various aspects of the risk or different risk factors.

Option B is incorrect because the roles required to be assigned to a Risk Response task may vary based on the configuration and complexity of the task. The 'risk_manager' role is not necessarily required; it might be a lower-level role that is assigned depending on the specific business needs.

Option C is incorrect because the "risk_admin" role is not required to assign the Risk Response task. A user with appropriate permissions, such as a risk owner or risk analyst, might be able to assign the task, depending on the system's configuration. The workflow, not a specific role, drives the task.

In summary, ServiceNow uses workflows to ensure consistent and automated progression of Risk Response tasks. This removes manual intervention and provides a streamlined process.

Relevant Documentation:

ServiceNow Risk Management: https://docs.servicenow.com/bundle/utah-governance-risk-compliance/page/product/grc/concept/risk-management.html
ServiceNow Workflow: https://docs.servicenow.com/bundle/utah-platform/page/administer/workflow/concept/workflow.html

Question: 5

What table, along with the Policy table, is linked to the Control Objective table by a many-to-many relationship?

A.Entity Class
B.Citation
C.Authority Documents
D.Risk Framework

Answer: B

Explanation:

Here's a detailed justification for why the correct answer is **B. Citation**, along with authoritative links for further research:

The Control Objective table in ServiceNow's Risk and Compliance application establishes many-to-many relationships with both the Policy and the Citation tables. This means a single Control Objective can be related to multiple Policies and multiple Citations, and vice-versa.

Why Citation? Citations represent specific clauses, sections, or references within external Authority Documents or internal Policies that a Control Objective is designed to satisfy or comply with. Think of citations as the granular pieces of legal text, standards, or frameworks. Each control objective might refer to several citations spanning multiple authoritative sources. For example, a control objective focused on data encryption could cite a specific clause in GDPR and a section from a NIST cybersecurity framework. Therefore, a many-to-many relationship is suitable because one citation can be related to multiple control objectives, and one control objective may require compliance with multiple citations.

Why not Entity Class? Entity Classes are used to categorize different types of entities within an organization, such as business processes, applications, or systems. While Control Objectives are associated with Entities (through the Entity Type and Entity fields), the relationship is not a many-to-many link via a separate table. It's more of a direct association.

Why not Authority Documents? Authority Documents are related to Citations. The relationship between

Control Objective and Authority Documents is indirect, achieved via the Citation table which links the Control Objective to the specific part of the Authority Document.

Why not Risk Framework? While Risk Frameworks are related to Policies, which are then connected to Control Objectives, the Risk Framework is not directly linked to the Control Objective through a many-to-many relationship. Instead, the Risk Framework influences the policies.

In summary, the Citation table serves as the crucial intermediary, creating a many-to-many link between Control Objectives and the specific regulatory, legal, or policy requirements they address. The many-to-many relationship is fulfilled by a table joining the two others (Citation and Control Objective), where you create relationships between them.

Here are some authoritative links:

1. **ServiceNow Product Documentation - GRC:** This is the primary source for understanding ServiceNow's GRC capabilities. While specific table relationships might not always be explicitly diagrammed, exploring the documentation on Policies, Control Objectives, and Citations will reveal their interdependencies.

   Search ServiceNow Docs for "GRC Control Objective," "GRC Policy," and "GRC Citation."

2. **ServiceNow Community Forums:** The ServiceNow community is a valuable resource for asking questions and finding solutions related to ServiceNow implementations. Search for discussions about the relationships between Policies, Control Objectives, and Citations.

   ServiceNow Community

By examining these resources, you can gain a comprehensive understanding of the relationships between these tables and how they contribute to the overall functionality of ServiceNow's GRC module.

Question: 6

Why would you create Entity classes?

A.To show relationships between tables or objects you are tracking that doesn’t otherwise exist anywhere in ServiceNow

B.To be assigned to risk statements, which generate risks for every Entity listed in the Entity Class

C.To be assigned to Control Objectives, which generate Controls for every Entity listed in the Entity class

D.To show relationships between Entities and Policies and map them directory to Citations

Answer: A

Explanation:

The correct answer is **A. To show relationships between tables or objects you are tracking that doesn’t otherwise exist anywhere in ServiceNow.**

Here's a detailed justification:

Entity Classes in ServiceNow's Risk and Compliance module serve as a way to represent a group or classification of Entities. Entities represent specific objects (applications, servers, databases, business processes, etc.) that are subject to risks and controls. While ServiceNow inherently has relationships between various tables (e.g., business application to server), Entity Classes are specifically helpful when you need to define new or custom relationships that aren't already modeled within the platform's standard data model.

Options B and C are incorrect because while Entity Classes are used in conjunction with Risk Statements and Control Objectives, they don't directly generate Risks or Controls for every Entity listed. You would need to associate specific Entities to Risk Statements or Control Objectives for the controls/risks to become applicable. Entity Classes help in efficient association by providing a mechanism to quickly apply these to a group.

Option D is also incorrect. While relationships between Entities and Policies exist and can be mapped (and the Policy module does use Citations), Entity Classes primarily exist for defining broader relationships between entities which may then be used to link to Policies. The core purpose isn't to directly map Entities to Citations.

In essence, Entity Classes fill the gap when the standard ServiceNow data model doesn't fully capture the relationships between the objects that are relevant to your organization's risk and compliance posture. They are a powerful tool for categorizing entities and defining new organizational structures for risk management.

For further research and authoritative information:

ServiceNow Documentation on Entity Classes: While direct links to specific ServiceNow documentation on Entity Classes are difficult to maintain due to ServiceNow's frequent updates, a search within the ServiceNow product documentation (accessible with a ServiceNow instance) for "Entity Class" and "GRC" (Governance, Risk, and Compliance) will yield the most current information.

Question: 7

The Tablename.config:

A.Displays the configuration list view of the table in the browser tab
B.Displays the table in list view within the Content Frame
C.Displays the table in list view within a separate browser tab
D.Displays the configuration list view of the table in the Content Frame

Answer: D

Explanation:

The correct answer is D because Tablename.config in ServiceNow typically refers to a way to access the configuration list view of a specific table within the platform. The configuration list view allows administrators and developers to see and manage configuration details related to that table, such as UI policies, client scripts, business rules, and other customizations. Because ServiceNow applications run within a browser, accessing Tablename.config usually presents the configuration information within the ServiceNow user interface, not in a new browser tab or separate window (which options A and C suggest). The main user interface area where ServiceNow displays information is often called the Content Frame. Therefore, displaying the configuration list view of the table in the Content Frame accurately describes the effect of Tablename.config. Option B is incorrect as it does not display configuration information, but instead only shows a listing of the table's records.

The Tablename.config is a shortcut to access the configuration record list, which is extremely helpful for developers and administrators. This allows easy navigation to table-specific configurations and helps when debugging or understanding how a table is configured. Direct links to configurations improve workflow by avoiding the need to search for configurations through various system administration modules. It efficiently displays the configurations in the main content area, aligning with ServiceNow's user interface design.

For further research on ServiceNow table configurations and UI navigation, refer to the official ServiceNow documentation. While a specific page about Tablename.config might not exist as it's a direct URL convention, understanding table administration and UI elements is crucial. Look into topics such as:

"System Definition > Tables"
"UI Policies"
"Client Scripts"
"Business Rules"

These resources on the ServiceNow documentation site will provide a deeper understanding of how tables are structured and configured within the ServiceNow platform. Understanding the relationship between tables and associated UI elements is fundamental to effective ServiceNow development and administration.

Question: 8

Which of the following extends from items?

A.Citation
B.Controls
C.Issue
D.Policy

Answer: B

Explanation:

The correct answer is **B. Controls**. Here's a detailed justification:

In ServiceNow's Risk and Compliance application, several tables extend from the GRC: Item table.
Understanding this hierarchy is crucial for implementation and customization. Controls directly relate to managing risks and ensuring compliance by implementing specific measures. These measures are documented and managed within the 'Controls' table, which inherits attributes and functionalities from the base 'Item' table. This inheritance allows for standardized data structures, workflow management, and reporting across different compliance areas.

A control is a preventative or detective measure implemented to mitigate a risk and enforce compliance with policies, regulations, or standards. Because a Control is something that is actively performed it inherits from the Item.

Citations are more about referencing rules or regulations. Issues represent problems or gaps found during audits or assessments. Policies outline organizational standards or requirements. While Issues and Policies might indirectly relate to items, they don't directly extend from the Item table in the same way Controls do.
Issues generally relate to remediation tasks. Policies may have items such as citations that must be implemented.

The Item table provides the basic structure for all record types within the Risk and Compliance application.
The Control table inherits common attributes such as description, assigned to, and state, but also adds specialized fields related to control objectives, test plans, and effectiveness assessment. This specialized extension makes Controls the most appropriate answer in the context of ServiceNow's Risk and Compliance architecture.

Therefore, the Control record is where you are creating, managing, and performing some task, which an item is most closely related to.

For further research, you can refer to the official ServiceNow documentation on the GRC application:

ServiceNow GRC Overview: https://www.servicenow.com/products/governance-risk-compliance.html ServiceNow Documentation (search for GRC tables and hierarchy): https://docs.servicenow.com/ (Requires

ServiceNow login)

Specifically, search the ServiceNow documentation for "GRC Data Model" to see the relationships between tables within the GRC module. This will help clarify the inheritance structure and the role of the Item table.

Question: 9

What happens when you assign an Entity Type to a Risk Statement?

A.An assessment will be automatically generated to test each Entity listed in the Entity Type
B.A risk assessment is created automatically for every Entity listed in the Entity Type
C.A risk is automatically generated for every Entity listed in the Entity Type
D.The Entity is now going to present a risk score and controls are going to be tied to it

Answer: C

Explanation:

Here's a detailed justification for why answer C is the correct choice, explaining the relationship between Entity Types, Risk Statements, and Risks in ServiceNow GRC:

The core principle here lies in understanding how ServiceNow's Risk and Compliance application models risk. A Risk Statement represents a generalized potential risk. When you associate an Entity Type with a Risk Statement, you're essentially saying, "This risk statement applies to all Entities of this type."

Answer C, "A risk is automatically generated for every Entity listed in the Entity Type," accurately reflects this. When you assign an Entity Type to a Risk Statement, the system automatically creates individual Risk records for each Entity within that Entity Type. Each Risk record will then inherit properties from the linked Risk Statement, giving you a concrete, instance-level risk assessment for each affected Entity. This is how ServiceNow operationalizes risk management, moving from a general statement to tangible instances of risk impacting specific entities. This is crucial for assigning ownership, tracking remediation efforts, and calculating risk scores at the individual entity level.

Now, let's examine why the other options are less accurate.

A. An assessment will be automatically generated to test each Entity listed in the Entity Type: While assessments are related, they are not automatically triggered by the initial assignment of an Entity Type to a Risk Statement. Assessments are typically initiated based on a defined schedule or other triggering events, and they test the risk, not directly represent it.

B. A risk assessment is created automatically for every Entity listed in the Entity Type: This is close, but subtly incorrect. It creates risks not an independent risk assessment record.

D. The Entity is now going to present a risk score and controls are going to be tied to it: This is partially true as Risk scores would subsequently be related to the Entity when a Risk is associated with it.

Therefore, only option C accurately captures the immediate outcome of associating an Entity Type with a Risk Statement.

Here are some relevant links for further research:

ServiceNow Docs - Risk Management:https://docs.servicenow.com/bundle/vancouver-governance-risk-compliance/page/product/risk-management/concept/risk-management-overview.html
ServiceNow Community Forums - Risk Management: Search the ServiceNow Community for discussions and examples related to Risk Statements and Entities.

Question: 10

There is a direct relationship between Entity Class and Entity Type when:

A.They have the same Entity Types
B.There is no direct relationship
C.They have the same Entities
D.They leverage the same reporting

Answer: B

Explanation:

The correct answer is **B. There is no direct relationship**.

Here's why:

In ServiceNow's Governance, Risk, and Compliance (GRC) module, specifically within Risk and Compliance, Entity Class and Entity Type serve distinct purposes related to organizing and categorizing entities (like applications, systems, or business processes) that are subject to risk assessments, controls, and compliance requirements.

An **Entity Class** is a high-level grouping of entities, often reflecting organizational departments or functional areas (e.g., "IT," "Finance," "Human Resources"). It provides a broad classification mechanism. Think of it as the top level of a classification hierarchy.

An **Entity Type** defines the specific nature of the entity (e.g., "Server," "Database," "Application," "Policy"). It provides a more granular categorization within an Entity Class. For example, within the "IT" Entity Class, you might have Entity Types like "Server" or "Database."

While an Entity Type is associated with an Entity Class (you select the Entity Class when creating or configuring an Entity Type), there isn't a direct, fixed relationship enforcing that they must share the same types or entities. The purpose of defining both is to allow for flexible categorization. You can have different Entity Types within the same Entity Class, and an Entity Type can even (though not best practice in most scenarios) be associated with multiple Entity Classes. The relationship is hierarchical, not directly equivalent. They do not need to have the same entities, and leveraging the same reporting is more of a consequence of their association than a direct relationship driver.

Therefore, the statement that there is a direct relationship between Entity Class and Entity Type when they have the same Entity Types or Entities, or leverage the same reporting is incorrect. The relationship is about classification and association within the GRC framework, not direct equivalence. The association facilitates hierarchical organization, rather than demanding identical contents or types.

Useful links (while not a direct "Servicenow documentation" link to the exact question, they help understand the relationship between entity classes and entity types):

ServiceNow GRC Overview: (Search on ServiceNow docs for) "Governance, Risk, and Compliance (GRC)" to understand the general context.
ServiceNow Entity Management: (Search on ServiceNow docs for) "GRC Entity Management" to explore the role of entities in GRC.

Question: 11

Which filter navigation syntax displays the table in list view within a separate browser tab?

A.Tablename_LIST
B.Tablename.list
C.Tablename.LIST
D.Tablename.List

Answer: C

Explanation:

The correct answer is C, Tablename.LIST, because ServiceNow filter navigation syntax is case-sensitive, especially concerning keywords like LIST. When the keyword LIST is entirely in uppercase and appended to the table name with a dot (.), ServiceNow interprets this as an instruction to display the list view of that table in a new browser tab.

Option A, Tablename_LIST, uses an underscore instead of a dot, which is incorrect syntax for this purpose. Option B, Tablename.list, uses lowercase list, which won't trigger the desired behavior of opening in a new tab; it may display the list in the current frame if the user has sufficient permissions. Option D, Tablename.List, uses only the first letter as uppercase and it will have similar behavior as tablename.list. In essence, Tablename.LIST is a specific command understood by the ServiceNow platform to handle the list view request in a particular manner. The capitalized LIST acts as a signal to create a separate browsing context.

Using the correct syntax is crucial because ServiceNow's URL routing and navigation heavily rely on precise naming conventions. The system parses the URL based on these conventions to determine which modules, tables, and views to load. Deviations from these conventions will likely lead to errors, incorrect page rendering, or unintended behavior.

Refer to the official ServiceNow documentation on navigating using filter navigation for more in-depth explanation on syntax rules and the behavior of various URL commands:

ServiceNow Docs on Lists: https://docs.servicenow.com/bundle/sandiego-platform-administration/page/user-interface/lists/concept/c_Lists.html (This link provides general information about lists in ServiceNow, which is the view being accessed.)

ServiceNow Community Forums: The ServiceNow community forums often contain discussions and examples related to filter navigation and URL syntax. Searching for terms like "ServiceNow filter navigation LIST" will likely yield helpful threads.

Question: 12

Jim is an Audit Manager. In addition to Audit Manager, which roles should be assigned to ensure he can manage the audit process as well as other GRC functions related to audit? (Choose two.)

A.sn_grc.manager
B.sn_audit.user
C.sn_grc.user
D.sn_grc.reader
E.sn_grc.developer

Answer: AB

Explanation:

The correct answer is **A. sn_grc.manager** and **B. sn_audit.user**.

Let's break down why:

sn_grc.manager: This role provides Jim with the necessary permissions to manage the overall GRC (Governance, Risk, and Compliance) processes within ServiceNow. It typically grants access to configure GRC modules, manage policies, risks, and controls, and oversee the broader GRC framework. An audit manager needs this higher-level GRC management capability to coordinate audit findings with the overall risk and compliance posture of the organization.

sn_audit.user: This role is specifically related to the Audit Management application. It gives Jim the ability to create, manage, and track audits. As an Audit Manager, this is a fundamental role because it allows him to directly interact with the audit records, assign tasks to auditors, review findings, and generate reports. It provides the specific functionality to manage the audit lifecycle.

Why the other options are incorrect:

C. sn_grc.user: This role provides basic access to GRC functionalities but doesn't grant the elevated privileges needed for management. It is suitable for users who need to view GRC records or perform basic tasks.

D. sn_grc.reader: This role is read-only access to GRC data. It's suitable for stakeholders who need to be informed but not actively involved in managing GRC processes.

E. sn_grc.developer: This role is for developers who need to customize and extend the GRC application. It is not relevant to the responsibilities of an Audit Manager.

In essence, Jim needs the "sn_grc.manager" role to orchestrate GRC functions related to audit and the "sn_audit.user" role to manage the audit process itself. This combination enables him to fulfill his responsibilities effectively within the ServiceNow environment.

Question: 13

What table extends from Document Table?

A.Risk
B.Risk Framework
C.Risk Response Task
D.Risk Statement

Answer: B

Explanation:

The correct answer is **B. Risk Framework**. Here's a detailed justification:

In ServiceNow's Risk and Compliance application, the Document table serves as a foundational base table for various records that require document management capabilities, such as attachments, versions, and approvals. Tables extending from the Document table inherit these functionalities.

Risk Framework stores the parent framework of a Risk. A Risk Framework, by its nature, needs to be documented comprehensively, often requiring attachments, version control (as the framework evolves), and approval workflows for changes. Therefore, the Risk Framework table extends the Document table to inherit these document-centric functionalities.

Let's examine why the other options are less likely:

A. Risk: While risks often have associated documentation, the core data structure of a risk record itself is not primarily focused on document management. The Risk table itself might be indirectly associated with documents, but not extend the document table directly. It is likely to be related to risk events that contain documents.

C. Risk Response Task: These tasks represent actions taken to mitigate risks. Like risks, these tasks might have related documents, but the table itself doesn't need to inherit all functionalities of the document table.

D. Risk Statement: These are descriptions of the identified risk. While they might form a part of a Risk Framework, they would most likely live within a Risk record and not inherit from the document table.

In conclusion, Risk Framework is best suited to inherit from the Document table. This allows for efficient management of the documents and versions necessary for such frameworks within ServiceNow.

Authoritative Links:

ServiceNow Product Documentation (search for "Document Table" and "Risk Framework" within ServiceNow docs): https://docs.servicenow.com/

Question: 14

Which of the following are scoped applications related to the Risk and Compliance applications? (Choose four.)

A.GRC: GRC Profiles
B.GRC: Attestation Design
C.GRC: UCF Compliance
D.GRC: Policy and Compliance
E.GRC: Performance Analytics
F.GRC: Risk Management

Answer: ACDF

Explanation:

The correct answer identifies four scoped applications closely related to ServiceNow's Risk and Compliance suite. Here's why:

A. GRC: GRC Profiles: This application manages profiles of entities (users, departments, locations, assets) within the organization. These profiles are foundational for associating risks, controls, and policies to specific areas, driving the risk management process within the ServiceNow ecosystem. This is an essential part of risk assessment and helps in the organization and navigation of risk information.

C. GRC: UCF Compliance: This application integrates with the Unified Compliance Framework (UCF), providing a comprehensive library of regulatory and industry standards. It enables organizations to map controls to multiple regulations, simplifying compliance efforts and reducing redundancy. Leveraging UCF accelerates the compliance process by providing standardized mappings.

D. GRC: Policy and Compliance: This is a core application within the Risk and Compliance suite. It manages policies, standards, and regulatory requirements. It facilitates the creation, distribution, and attestation of policies, ensuring employees are aware of and compliant with organizational guidelines. This is fundamental for establishing a strong risk and compliance framework.

F. GRC: Risk Management: This application focuses on identifying, assessing, and mitigating risks. It supports risk assessments, risk registers, control testing, and remediation efforts. This is central to any Risk and Compliance program within ServiceNow. This application drives the overall risk lifecycle.

B. GRC: Attestation Design is related to the overall GRC suite, and while important in compliance programs, it is generally considered a part of the larger Policy and Compliance management process rather than a separate, foundational scoped application on par with the others.

E. GRC: Performance Analytics while often used with Risk and Compliance to visualize and monitor key metrics, it is a separate, broader application that isn't specific to Risk and Compliance.

Further Research:

ServiceNow Documentation: Search the ServiceNow documentation portal (requires ServiceNow instance access or account) for "Risk Management," "Policy and Compliance," "GRC Profiles," and "UCF Compliance" for in-depth information on each application.

Question: 15

Which tables extend the Content (sn_grc_content) table? (Choose two.)

A.sn_compliance_citation
B.sn_grc_issue
C.sn_compliance_policy_statement
D.sn_risk_risk

Answer: AC

Explanation:

The correct answer is A. sn_compliance_citation and C. sn_compliance_policy_statement.

The Content (sn_grc_content) table in ServiceNow serves as a central repository for various types of GRC content. To determine which tables extend it, you need to examine the ServiceNow data model, specifically the inheritance hierarchy. Tables that extend the Content table inherit its fields and functionalities and add their own specific attributes.

A. **sn_compliance_citation:** This table stores citations that are relevant to compliance requirements. Citations can provide evidence or context for a control's effectiveness. Because citations need to be centrally managed and related to other GRC elements, it makes sense to have them inherit from the Content table.

C. **sn_compliance_policy_statement:** Policy statements are core components of a compliance program. They articulate the organization's stance on particular topics related to risk and compliance. Like citations, policy statements benefit from centralized content management, so they inherit from the Content table.

B. **sn_grc_issue:** While issues are a core component of GRC, they track problems or exceptions related to controls or compliance. They represent occurrences that need to be addressed. Issues are typically associated with Controls and Tasks, but they don't directly represent content in the same way as citations or policy statements. Therefore, they don't inherit from the Content table directly. Instead, they may relate to content stored in the Content table through relationships.

D. **sn_risk_risk:** Risks represent potential threats to the organization. While they are a core part of GRC, they don't directly represent content in the same way as citations or policy statements. Risk records capture information about potential negative impacts, likelihood, and vulnerabilities, and although risks can certainly relate to compliance policy, they don't extend the content table. They are generally related to controls or risk statements.

In summary, the sn_compliance_citation and sn_compliance_policy_statement tables directly extend the Content (sn_grc_content) table because they manage specific types of GRC content that benefit from

centralized content management.

Relevant ServiceNow documentation can be found by searching for "GRC data model" or individual table names in the ServiceNow documentation portal.

Question: 16

All of the following are PARENT tables which exist within the GRC Entities application scope EXCEPT.

A.Item
B.Document
C.Content
D.Indicator

Answer: D

Explanation:

Here's a detailed justification of why the correct answer is D, Indicator, and why the others are incorrect in the context of ServiceNow GRC Entity parent tables:

The question focuses on identifying a table not considered a parent table within the GRC Entities application scope in ServiceNow. Parent tables are fundamental tables that other tables extend from, inheriting their fields and properties. Within GRC, the Entity domain needs to model diverse elements, and parent tables provide the foundation for specialization.

Item (A): The Item table is a parent table commonly extended by other tables within the GRC Entities application scope. Items represent a generalizable object or element tracked within GRC processes.

Document (B): The Document table is also a standard parent table. Numerous records within GRC, such as policies, procedures, and evidence, are often stored as or linked to document records. Thus, tables associated with those items often extend Document.

Content (C): The Content table serves as another parent table. It could represent various forms of content, such as knowledge base articles or snippets of text used in policies, that various other tables rely upon and extend.

Indicator (D): The Indicator table, unlike the others, is generally not a direct parent table for Entities. Indicators are primarily linked to control objectives or used to measure compliance performance. While an entity can be associated with indicators, the Indicator table doesn't typically function as a direct parent table from which entity records inherit. Indicators are often used for compliance measurement but do not themselves serve as a base table extended by various entity types.

Therefore, the correct answer is **D, Indicator** as it is the least likely table to function as a parent table to tables within the GRC Entities application scope.

Reference link: https://docs.servicenow.com/ (Servicenow Documentation - Navigate to GRC section)

Question: 17

Which table stored the links from Entity to Entity Types?

A.[sn_compliance_m2m_profile_profile_type]

B.[sn_risk_m2m_risk_profile]
C.[sn_compliance_m2m_policy_profile]
D.[sn_grc_m2m_profile_profile_type]

Answer: D

Explanation:

The correct answer is **D. [sn_grc_m2m_profile_profile_type]**. This table is explicitly designed within ServiceNow's Governance, Risk, and Compliance (GRC) module to manage the many-to-many relationships between Entities (Profiles) and Entity Types (Profile Types). This relationship is crucial for categorizing and classifying different types of entities within the GRC framework, such as organizations, systems, or processes.

The table name itself hints at its purpose: sn_grc indicates it's part of the GRC application, m2m signifies a many-to-many relationship, profile_profile_type denotes the connection between profiles (entities) and profile types (entity types). This structure allows each entity to be associated with multiple entity types, and each entity type can be linked to multiple entities.

Options A, B, and C, while also M2M tables, relate to different specific relationships within ServiceNow: Compliance and Risk. They don't specifically manage the fundamental linking of entities to their overarching types as directly as sn_grc_m2m_profile_profile_type. Option A focuses on Compliance Profiles to Profile Types, option B on Risk Profiles, and option C on Policy Profiles. While Profiles might act as Entities, they are contextually bound to specific areas (Compliance, Risk, Policy). In contrast, sn_grc_m2m_profile_profile_type serves as a general purpose mapping table at a higher abstraction level.

Therefore, when needing to identify the table linking entities to entity types in the broader GRC context, sn_grc_m2m_profile_profile_type provides the most accurate and direct connection.

Further research can be done on the ServiceNow documentation site specifically looking at the GRC data model. While a direct page explicitly stating this exact table and this exact purpose might be difficult to find, exploring the relationships around the Profile and Profile Type tables within the GRC data model will clarify its role. Also, searching for "[sn_grc_m2m_profile_profile_type] servicenow" in the ServiceNow community forums might yield more specific examples.

Question: 18

Where does a policy get published to when it is approved?

A.Knowledge Summit
B.ServiceNow Library
C.Authoritative Records
D.Knowledge Base

Answer: D

Explanation:

The correct answer is **D. Knowledge Base**.

When a policy is approved in ServiceNow's Risk and Compliance application, it is published to the Knowledge Base. This is because the Knowledge Base serves as the central repository for documented information, processes, and policies within an organization. Publishing to the Knowledge Base ensures that the policy is readily accessible to relevant stakeholders for reference and consumption. Options A, B, and C are incorrect

because they do not represent the standard repository or publication destination for policies within the ServiceNow Risk and Compliance framework. The Knowledge Summit and ServiceNow Library are not relevant terms within this context. Authoritative Records could potentially be part of the governance model, but the approved policy document itself is centrally accessible via the Knowledge Base. The goal is to make the policy easily searchable and available to employees who need to understand and adhere to it. The ServiceNow platform uses the Knowledge Base to manage and distribute information effectively, promoting policy awareness and compliance. By centralizing policies in the Knowledge Base, organizations can easily maintain version control, track usage, and facilitate updates, ensuring that the latest information is always available. This also streamlines the process of communicating changes to policies, improving overall compliance and reducing risk. The Knowledge Base empowers organizations to promote transparency and accountability by making key policies accessible to all relevant employees. This contributes to a stronger governance posture and a more compliant environment.

Reference link: (Refer to ServiceNow official documentation on Risk and Compliance and Knowledge Management)

Question: 19

What GRC module would you access in order to update Entity Types?

A.Risk > Entities
B.Scoping > Profiles
C.Scoping > Entity Types
D.CMDB

Answer: C

Explanation:

The correct answer is **C. Scoping > Entity Types**.

Here's why:

Entity Types in ServiceNow GRC (Governance, Risk, and Compliance) define the classification and characteristics of the objects that are being governed. These could represent business units, applications, processes, or IT assets.

The **Scoping** application within GRC is specifically designed to manage the definition and configuration of these entities, including their types. It provides the tools to define entity types, their associated attributes, and their relationships to other GRC objects.

Within **Scoping**, the **Entity Types** module provides the interface for creating, modifying, and managing these definitions. This is the direct path to updating Entity Types.

Option A (**Risk > Entities**) is incorrect because while you interact with entities within the Risk application, this is where you use entities, not define their types. The entity definition must exist before you start associating entities with risks.

Option B (**Scoping > Profiles**) is about configuring scoping profiles which automate the process of associating entities to policies and controls using a predefined criteria. This is not the place to edit the actual definition of entity types.

Option D (**CMDB**) is related to IT asset management, but is not directly connected to the GRC module for managing entity types related to compliance or risk. While CMDB data can be imported/integrated to GRC, the

module is not the correct path to change Entity Types.

Therefore, navigating to **Scoping > Entity Types** is the correct method for updating Entity Types in ServiceNow GRC.

Authoritative Links:

ServiceNow Documentation: Access Control List rules for Scoping https://docs.servicenow.com/bundle/tokyo-platform-administration/page/administer/security/reference/r_AccessControlRulesForGRC.html

Question: 20 The ServiceNow Platform requires which external components in order to ingest data from other systems?

A.The platform includes an SDK template that allows developers to enhance it using Java
B.A messaging bus needs to be developed
C.The platform allows XML to be ingested, and it required developers to leverage XSLT to map it properly D.The platform has Integration Service that allow users and developers to ingest data from a variety of sources

Answer: D

Explanation:

D. The platform has Integration Service that allow users and developers to ingest data from a variety of sources

The ServiceNow Platform provides built-in Integration Services (such as IntegrationHub) that enable users and developers to easily ingest data from many external systems and data sources, including REST APIs, SOAP web services, JDBC databases, and more.

These services provide connectors, data transformation, and orchestration capabilities without the need to build custom messaging buses or manually write complex mapping logic.

The platform supports multiple protocols and formats out of the box.

Question: 21 You are working with your customer to determine necessary audit management workflow configurations. What should they know about the approval process for audit engagements? (Choose three.)

A.If the engagement is approved and there are remaining open tasks or issues, it automatically moves into the Follow Up state.

B.If the engagement is approved and there are no remaining open tasks or issues, it automatically moves into the Closed state.

C.If the engagement is rejected, it automatically moves back to the Fieldwork state.

D.If the engagement is approved and there are remaining open tasks or issues, it automatically moves into the Fieldwork state.

E.If the engagement is rejected, it automatically moves into the Scope state.

Answer: ABC

Explanation:

The provided answer (ABC) is the most voted and aligns with the typical ServiceNow Risk and Compliance

Audit Management workflow. Let's break down each statement:

A. If the engagement is approved and there are remaining open tasks or issues, it automatically moves into the Follow Up state. This is generally true. Audit engagements often involve multiple tasks and findings. Upon approval, the workflow needs to track and manage these open items, hence moving to a "Follow Up" state to ensure they are addressed. This aligns with the concept of continuous monitoring in compliance.

B. If the engagement is approved and there are no remaining open tasks or issues, it automatically moves into the Closed state. This is also generally correct. Once an audit engagement has been approved and all tasks/issues have been resolved, there is no need for further active management. The engagement can be closed, signifying completion and adherence to compliance requirements.

C. If the engagement is rejected, it automatically moves back to the Fieldwork state. This statement requires more nuance but can be logically inferred from the context. While rejection might suggest a return to the "Scope" stage for fundamental re-evaluation, moving back to "Fieldwork" implies that the data collected during the fieldwork wasn't sufficient or accurate for the audit to be approved. This necessitates further data gathering and analysis, thus warranting a return to the "Fieldwork" stage to correct those deficiencies. In ServiceNow, a rejected engagement usually implies a need to fix errors in the already obtained data, hence reverting to a "Fieldwork" stage could be appropriate.

D. If the engagement is approved and there are remaining open tasks or issues, it automatically moves into the Fieldwork state. This statement is incorrect. If an engagement is approved, it's beyond the fieldwork state. Remaining tasks or issues will push it into the Follow-up stage.

E. If the engagement is rejected, it automatically moves into the Scope state. While revisiting the scope could happen after a rejection in certain situations, statement C is more directly relevant to the workflow, particularly in the context of fixing specific data inaccuracies or omissions uncovered during the Fieldwork. Rejection often requires correcting existing data/evidence and thus the direct return to the "Fieldwork" state is an intended functionality. Re-scoping may happen eventually, but will not be the first logical step.

In summary, options A, B, and C accurately describe standard workflow behaviors for audit engagements within a Risk and Compliance system. This is due to their reliance on the workflow transitioning, based on approval and task resolution. Rejecting audit engagements needs either more fieldwork to correct the data collected, or a re-scoping. Option C suggests a more immediate course of action, and thus, is the correct one.

Question: 22

Which GRC application would you use to manage internal or external consultancy processes that aim to prove the effectiveness of controls?

A.Audit Management
B.Risk Management
C.Vendor Risk Management
D.Policy and Compliance Management

Answer: D

Explanation:

The correct answer is **D. Policy and Compliance Management**. While Audit Management (A) might seem relevant, it's typically used after controls are implemented to verify their effectiveness. Risk Management (B) focuses on identifying, assessing, and mitigating risks, not specifically on proving control effectiveness. Vendor Risk Management (C) deals with risks associated with third-party vendors.

Policy and Compliance Management is the most appropriate choice because it directly deals with establishing and maintaining policies and controls to meet compliance requirements. Consultancies often work to assess and improve policies and control frameworks to ensure they are effective in meeting these requirements. Activities like control testing, gap analysis, and remediation planning, aimed at proving control effectiveness, fall squarely within the Policy and Compliance Management domain. The consultancy process ultimately aims to enhance the organization's compliance posture, which is managed within this application.

In the context of demonstrating control effectiveness, Policy and Compliance Management supports activities such as:

Defining and documenting policies and procedures.
Mapping policies to relevant regulations and standards.
Assessing the design and effectiveness of controls.
Managing exceptions and remediation plans.
Tracking compliance status.
Providing evidence of compliance to auditors and regulators.

Therefore, for managing consultancy processes aimed at proving the effectiveness of controls and bolstering overall compliance, the Policy and Compliance Management application is the most suitable choice.

Relevant links for further research:

ServiceNow Policy and Compliance Management: https://www.servicenow.com/products/policy-compliance-management.html
ServiceNow Governance, Risk, and Compliance (GRC): https://www.servicenow.com/solutions/governance-risk-compliance.html

Question: 23

What are the Risk Scoring methods available in ServiceNow? (Choose two.)

A.Quantitative
B.Qualitative
C.Inherent
D.Residual
E.Calculated

Answer: AB

Explanation:

The correct answer is A and B: Quantitative and Qualitative.

ServiceNow's Risk Management module focuses on assessing and managing risks, and the scoring methods are crucial for prioritizing mitigation efforts. Risk scoring involves determining the level of risk associated with a specific entity, process, or asset.

Quantitative risk assessment involves assigning numerical values to both the likelihood and impact of a risk. This method leverages data and statistical analysis to provide a more objective measure of risk. For example, the likelihood of a data breach might be quantified as a probability (e.g., 0.1 or 10%), and the impact might be quantified in monetary terms (e.g., $1 million in potential fines and damages). The risk score is then calculated based on these numerical inputs. This scoring method gives organizations better insight to compare risks.

Qualitative risk assessment, on the other hand, uses descriptive scales to evaluate the likelihood and impact of risks. Instead of assigning numerical values, risks are categorized using terms like "High," "Medium," or

"Low." This method relies on expert judgment and subjective assessments. While less precise than quantitative methods, qualitative assessment can be valuable when data is limited or unavailable. This scoring method is useful when you want to understand the risk without diving into the numbers.

Inherent risk and Residual risk are not Risk Scoring methods, but represent risk states. Inherent risk is the risk level before any controls are implemented, and Residual risk is the risk level after controls are in place. Calculated refers to automated risk calculations but it is not a risk scoring method.

Authoritative links:

ServiceNow Risk Management Documentation: (Search ServiceNow documentation portal for "Risk Management" to get the latest documentation, as URLs change frequently.)
NIST Risk Management Framework: https://csrc.nist.gov/projects/risk-management (although not ServiceNow specific, it provides a foundational understanding of risk assessment).

Question: 24

The Risk thresholds in the Risk Criteria Matrix (default values) do not line up with company needs. What should you do?

A.Configure the Risk Criteria in ServiceNow
B.Identify Risk that will benefit from the default values
C.Demonstrate Risk scoring scenarios using the default values
D.Use the default values to determine new company approach

Answer: A

Explanation:

The correct answer is A: Configure the Risk Criteria in ServiceNow.

Here's why: The purpose of a risk management framework, especially within a platform like ServiceNow's Risk and Compliance module, is to align with an organization's specific risk appetite and tolerance. Risk thresholds, defined in the Risk Criteria Matrix, are crucial elements of this framework. If the default values don't match the company's needs, it signifies a misalignment that must be addressed. Option A, configuring the Risk Criteria, directly tackles this misalignment by allowing you to customize the thresholds to reflect the organization's actual risk tolerance levels. This ensures accurate risk assessments and prioritization.

Options B, C, and D are not optimal. Simply identifying risks that fit default values (Option B) is a backward approach. The risk management system should adapt to the organization, not the other way around. Demonstrating risk scoring using defaults (Option C) is useful for understanding the system, but it doesn't address the core issue of misalignment with company needs. Using defaults to dictate a new company approach (Option D) is fundamentally flawed; the risk management framework should reflect the organization's established risk management strategy and objectives.

Customization is a key advantage of cloud-based platforms like ServiceNow. The ability to configure risk criteria empowers organizations to tailor the system to their specific context. The ServiceNow documentation itself encourages customization to ensure alignment with business requirements. Failure to adjust risk thresholds can lead to inaccurate risk assessments, misallocation of resources, and ultimately, ineffective risk management. In conclusion, tailoring the Risk Criteria Matrix is the appropriate action to ensure ServiceNow effectively supports the organization's risk management strategy.

Authoritative Links for further research:

ServiceNow Risk Management:https://www.servicenow.com/products/risk-management.html

ServiceNow Documentation - Risk Management:https://docs.servicenow.com/bundle/quebec-governance-risk-compliance/page/product/grc/concept/risk-management.html

Question: 25

Who can move a Policy into Review? (Choose two.)

A.sys admin
B.policy approver
C.policy reviewer
D.policy owner

Answer: BD

Explanation:

The correct answer identifies who can move a Policy into the 'Review' state within ServiceNow's Risk and Compliance module. A Policy moving into the Review state indicates a readiness to be examined and assessed for its effectiveness and adherence to organizational standards.

Option B, "policy approver," is correct. Policy Approvers are typically individuals with the authority to formally approve or reject a policy. They may initiate the review process before providing final approval to ensure the policy aligns with organizational goals and regulatory requirements.

Option D, "policy owner," is also correct. Policy Owners are responsible for the content, accuracy, and ongoing maintenance of a policy. They possess the knowledge to assess when a policy needs review due to changes in regulations, business processes, or internal audits. Therefore, they can initiate the review process.

Option A, "sys admin," is incorrect. While sys admins have broad system access, they are typically not responsible for the content or lifecycle of specific policies. Their role is more technical, focusing on system administration and maintenance, rather than policy governance.

Option C, "policy reviewer," is incorrect. While policy reviewers participate in the review process, they don't typically initiate it. Their role is to assess the policy after it has been put into the 'Review' state by the policy owner or approver. They provide feedback and suggestions for improvement.

In summary, the policy owner and policy approver are the most logical roles to initiate the 'Review' phase of a policy. The Policy Owner manages the content and knows when an update is needed, triggering the need for review. The Policy Approver, before final approval, might initiate a review to ensure everything is up to standard.

Further research on ServiceNow's Risk and Compliance modules can be found at:

ServiceNow Documentation:https://docs.servicenow.com/ (Search for "Policy and Compliance Management")
ServiceNow Community:https://community.servicenow.com/ (Search for discussions related to Policy and Compliance)

Question: 26

The Citation table is a child table of which parent?

A.Content
B.Authority Document

C.Item
D.Document

Answer: A

Explanation:

The correct answer is A, Content. Citations in ServiceNow GRC (Governance, Risk, and Compliance) directly relate to specific content. The Citation table (grc_citation) records evidence or references that support or refute assertions made within various GRC records. The "Content" field within the Citation table references the specific GRC record where the citation applies. It establishes a one-to-many relationship, meaning a single GRC record (the "Content") can have multiple Citations associated with it. This ensures traceability and provides documented proof for controls, risks, policies, and other GRC elements.

The other options are incorrect because Citations don't primarily link to them:

B. Authority Document: While Citations can reference Authority Documents, they are not the direct parent. Authority Documents provide the broader framework, but Citations point to specific sections within those documents or other GRC content.

C. Item: While some GRC objects might be considered items in a general sense, the "Item" table is not a direct parent for Citations in the context of standard ServiceNow GRC configurations.

D. Document: Similar to Authority Documents, while Citations can reference documents, the "Content" table acts as the more immediate parent, linking the Citation to the relevant record within the ServiceNow GRC module. The Content represents the target of the citation: where the reference will be displayed or will provide support.

In essence, the Citation table provides a mechanism to link evidence (the citation itself) to a specific piece of content within the GRC module, ensuring traceability and accountability. This aligns directly with core GRC principles of documented support for policies, controls, and risk assessments.

Authoritative Links:

While direct ServiceNow documentation links require a login, searching the ServiceNow documentation site for "GRC Citations" or "GRC Content Table" will provide detailed information on the tables and their relationships. Look for topics related to "GRC Data Model" and "GRC Tables".

Question: 27

Control Failure Factor represents the impact of Control Failures on what score?

A.Inherent
B.Residual
C.Total
D.Calculated

Answer: D

Explanation:

The answer is **D. Calculated**.

Here's a detailed justification:

In ServiceNow's Risk and Compliance application, Control Failure Factors directly influence the Calculated Risk Score. The application calculates risk scores dynamically, taking into account various factors, including the effectiveness of controls. When a control fails, the Control Failure Factor reflects the severity and impact of that failure. This factor is used in the overall risk calculation.

Specifically, the Calculated Risk Score represents the current, dynamic assessment of risk based on real-time data, including the effectiveness of controls (or lack thereof, as reflected by Control Failure Factors), the inherent risk score, and the risk appetite.

Inherent Risk refers to the risk level before any controls are implemented. Residual Risk is the remaining risk level after controls are implemented. Total Risk may be calculated as a sum of all identified risks but isn't directly influenced by the Control Failure Factor in the same manner. The Control Failure Factor serves as a modifier within the risk calculation formula. A high Control Failure Factor increases the calculated risk score, reflecting the increased exposure due to the failed control.

The calculated risk score can trigger workflows, alerts, and remediation tasks. Without the influence of control failure factors, the calculated risk score will not accurately reflect the current state of risk. ServiceNow's documentation, training materials, and community forums offer further information and examples of risk score calculations and their relationship to control failure factors.

Consider this formula as an example: Calculated Risk Score = Inherent Risk Score + (Control Failure Factor * Control Strength). This formula is illustrative and can be customized.The inclusion of a failed control factor will raise the calculated risk.Links:ServiceNow Risk Management: https://www.servicenow.com/products/risk-management.html (General overview; specific calculations are in product documentation)

ServiceNow Documentation (requires ServiceNow login): Access to detailed ServiceNow documentation, including risk score calculations, typically requires a ServiceNow account and login.

Question: 28

Which one of the following is not a trigger for issue creation?

A.Manual issue created by any manager or admin role as well as by audit user
B.Indicator failure
C.Risk assessment returns the inherent and residual risk impact as 'Very High'
D.Attestation returns the result as 'Not Implemented'
E.Control effectiveness is 'Ineffective' and the state of control test is 'Closed Complete'

Answer: C

Explanation:

The correct answer is **C. Risk assessment returns the inherent and residual risk impact as 'Very High'**.

Here's why:

Issues in ServiceNow GRC (Governance, Risk, and Compliance) are generally created when there's a deviation from expected compliance or a gap in controls. Options A, D, and E all represent such deviations.

A. Manual issue creation: This is a fundamental capability, allowing authorized personnel to log issues they identify.

D. Attestation returns the result as 'Not Implemented': This clearly indicates a failure to meet a compliance requirement, directly triggering an issue.

E. Control effectiveness is 'Ineffective' and the state of control test is 'Closed Complete': This signifies a control that isn't working properly, despite testing being completed, creating a gap that requires an issue to be raised.

B. Indicator failure: Failing an indicator showcases a measurable deviation, thus triggering an issue for remediation.

However, a **Risk assessment returning a 'Very High' risk impact** doesn't automatically create an issue. Risk assessments identify and evaluate risks; a high risk score simply flags an area requiring further attention and potential mitigation. The need to create an issue is dependent on the specific risk response plan. The high risk score itself does not inherently mean a compliance violation or control failure has occurred that requires issue creation. Further analysis is generally required to determine if the high risk has materialized into a specific problem requiring an issue to be raised. It may necessitate further investigation, acceptance of risk, or the creation of mitigation plans. The risk assessment outcome informs decisions, but it's not a direct trigger for issue creation in the same way that a control failure or failed attestation is.

Therefore, while a high-risk assessment score can lead to issue creation, it's not a direct trigger in the same manner as the other options.

Supporting Documentation:

Although not directly stating "risk assessment is not a trigger for issue creation," these articles highlight the typical issue creation mechanisms and demonstrate how risk assessments themselves are not explicitly mentioned as such triggers. It's implied that other triggers are more direct, while risk assessment findings necessitate further analysis before issue creation.

ServiceNow Product Documentation on Issues: https://docs.servicenow.com/en-US/bundle/sandiego-governance-risk-compliance/page/product/grc/concept/grc-issues.html
ServiceNow Community article on GRC Workflow: https://community.servicenow.com/community?id=community_article&sys_id=2f1e5287db6804d064e102d5ca96190a

Question: 29

GRC Options in Interactive Filters are only available through which feature?

A.GRC Filtering
B.Metrics Reporting
C.Performance Analytics
D.Trending Analytics

Answer: C

Question: 30

In which state can reviewers either send the Policy back to draft or forward it by requesting approval?

A.Retired
B.Published
C.Awaiting Approval
D.Review

Answer: D

Explanation:

The correct answer is D. Review.

The Review state in a ServiceNow Risk and Compliance policy workflow is specifically designed for reviewers to analyze the policy content. During this stage, reviewers have the responsibility to either approve the policy for further progression in the workflow or reject it if they find deficiencies or require modifications. If a reviewer deems the policy unsuitable for approval, they can send it back to the Draft state, allowing the policy owner to make necessary revisions based on the feedback. Conversely, if the reviewer finds the policy satisfactory and complete, they can forward it to the next stage in the workflow, which is typically the "Awaiting Approval" state. In this state, approvers with higher authority will perform the final review and grant official approval for the policy. The Retired and Published states generally do not allow reviewers to directly send the Policy back to Draft. Retired policies are no longer active, and Published policies are already in effect. The "Awaiting Approval" state is for approvers, not reviewers, to request changes.

ServiceNow Documentation on Policy and Compliance: (https://docs.servicenow.com/en-US/bundle/rome-governance-risk-compliance/page/product/grc/concept/grc-policy-compliance.html)

Question: 31

The Risk Scoring values are entered on the Risk Statement. What records inherits the values from the Risk Statement?

A.Risk Criteria Matrix
B.Risk Framework
C.Registered Risk
D.Risk Response Issue

Answer: C

Explanation:

The correct answer is C. Registered Risk. Here's why:

The core concept revolves around data inheritance and the relationship between Risk Statements and Registered Risks within the ServiceNow Risk Management application. Risk Statements define the inherent characteristics and potential impact of a risk, including the risk score derived from various factors. Registered Risks, on the other hand, represent specific instances of that risk occurring within an organization's operational context.

Registered Risks are created based on Risk Statements. When a Registered Risk is created from a Risk Statement, it inherits the risk scoring values (such as inherent risk score, impact, and likelihood) that are defined at the Risk Statement level. This inheritance ensures consistency and efficiency in the risk assessment process. Instead of re-evaluating the inherent risk for every instance, the initial assessment defined in the Risk Statement is propagated to the Registered Risks.

The Risk Criteria Matrix (A) defines the definitions of risk scores (e.g., what constitutes "high" impact), but it doesn't inherit values. The Risk Framework (B) is a broader construct that defines the overall risk management approach and structure, not individual risk scores. Risk Response Issue (D) is a record created in response to a registered risk and does not directly inherit the scoring values from the risk statement. Registered Risks are direct instances that inherit the values allowing a consistent and streamlined approach.

For more details, refer to ServiceNow's official documentation on Risk Management, specifically the sections detailing Risk Statements and Registered Risks, which elucidate the relationships and inheritance

mechanisms within the platform. Also review documentation about the ServiceNow Risk Management model.

Question: 32

Which of the following statements correctly describe the risk management lifecycle process?

A.Access, Identify and Plan, Control, Review
B.Control, Review, Assess, Identify and Plan
C.Identify and Plan, Assess, Control, Review
D.Identify and Plan, Review, Assess, Control

Answer: C

Explanation:

The correct sequence for the Risk Management Lifecycle, according to ServiceNow best practices and industry standards, is **C. Identify and Plan, Assess, Control, Review**.

Here's why:

1. **Identify and Plan:** This is the crucial initial stage. It involves identifying potential risks, defining the scope of risk management, establishing objectives, and developing a plan for managing risks. Without proper identification, you cannot effectively manage risks.

2. **Assess:** Once risks are identified, they must be assessed. This involves evaluating the likelihood and impact of each risk. Risk assessment helps prioritize which risks need the most immediate attention and resources. Quantitative or qualitative methods may be used.

3. **Control:** After assessment, control measures are put in place to mitigate or prevent identified risks. These controls could be preventive (designed to stop the risk from happening) or detective (designed to detect the risk after it has occurred). The control activities should align with the risk appetite.

4. **Review:** The final stage is continuous monitoring and review of the effectiveness of the control measures. This includes evaluating the implemented controls, identifying any new risks that have emerged, and making necessary adjustments to the risk management plan. The entire process is iterative and requires continuous improvement.

Options A, B, and D present an incorrect order. Access is not generally considered a core stage within the standard risk management lifecycle. The placement of Review and Control at different positions other than at the end of the lifecycle defeats the purpose of continuous monitoring and mitigation strategies.

Therefore, the cycle begins with identifying and planning, then assessing the risks, controlling or mitigating the risks, and finally, reviewing the process and controls for effectiveness.

For further reading:

NIST Risk Management Framework:https://csrc.nist.gov/projects/risk-management (Although this covers broader IT systems, the underlying principles are similar)
ISO 31000 (Risk Management): (While a paid standard, summaries and excerpts are widely available online) This is a globally recognized standard for risk management.

Question: 33

When calculating compliance scores, what is true about the weighting of Controls? (Choose two.)

A.Controls are not weighted equally by default

B.The weight cannot be changed

C.The default value is 10

D.The weight of the Control is set when the Control is created

Answer: CD

Explanation:

The correct answer is **C. The default value is 10** and **D. The weight of the Control is set when the Control is created.** Let's break down why:

Control Weighting in ServiceNow GRC: ServiceNow's Governance, Risk, and Compliance (GRC) module utilizes controls to manage and assess compliance. The impact of each control on the overall compliance score is determined by its weight. This allows for prioritizing controls based on their criticality.

Default Weight: By default, when a new control is created within ServiceNow GRC, it is assigned a weight of 10. This means that each control, unless otherwise specified, contributes equally to the overall compliance score based on its weight.

Control Weight Configuration: The weight of a control is not fixed and can be customized when the control is created, or subsequently edited. System Administrators or GRC administrators can adjust the weight field within the control record to reflect its importance.

Therefore, a control's weight is indeed set during its creation and is configured. The default value is 10. If A were true, then not all controls would have the same weight initially and C being true contradicts this. B is incorrect because control weight can be changed.

Reference Link:

ServiceNow Docs on Risk Management(Note: while the exact phrasing might vary based on ServiceNow version, the core principle of weighted controls remains consistent)

Question: 34

Which role(s) has the capability to create Policies? Choose two.)

A.Compliance Manager

B.Compliance admin

C.Compliance User

D.Risk Manager

Answer: AC

Explanation:

The correct answer is **A. Compliance Manager and C. Compliance User**. This is because the Compliance Manager and Compliance User roles are equipped with the necessary permissions and responsibilities to create policies within the ServiceNow GRC (Governance, Risk, and Compliance) module.

A **Compliance Manager** is a key role responsible for overseeing the overall compliance program. Their duties include defining compliance requirements, managing compliance activities, and creating policies to ensure adherence to regulations and standards. They are primarily responsible for developing and implementing the compliance framework. Therefore, the role naturally requires the ability to create and manage policies.

A **Compliance User** role also permits creating compliance policies to assist the compliance managers. While

Compliance Users might not have the same level of authority as Compliance Managers, they often contribute to the policy creation process. The Compliance User can also track the policy's progress and provide insights for future policy creation.

A **Compliance Admin** typically handles the administrative aspects of the GRC module, such as user management, configuration, and system setup. While vital for the system's smooth operation, their primary focus is not policy creation. The administrative role sets up the system and manages security but not policy creation.

A **Risk Manager**, while involved in risk assessment and mitigation, focuses on identifying, analyzing, and managing risks, not on creating compliance policies. Their efforts are distinct from the processes regarding compliance policy creation. The Risk Managers ensure risks are identified, accessed, and managed, and work separately from compliance policy management.

Here are authoritative links for further research:

ServiceNow Documentation: Roles in Governance, Risk, and Compliance:https://docs.servicenow.com/ (Search within the ServiceNow documentation for "GRC roles" to get the most relevant and up-to-date information).

ServiceNow Community Forums:https://community.servicenow.com/ (Search the forums for discussions related to GRC roles and permissions).

Question: 35

The 'Add to Update Set' utility is available for download via:

A.ServiceNow Developer site
B.ServiceNow store
C.ServiceNow Community
D.ServiceNow HI support

Answer: A

Explanation:

The correct answer is A: ServiceNow Developer site. The 'Add to Update Set' utility is specifically designed to streamline the process of capturing customizations within a ServiceNow instance and moving them between instances. This utility is intended for developers and administrators who are actively involved in building and configuring ServiceNow applications.

The ServiceNow Developer site (developer.servicenow.com) serves as the central hub for resources aimed at empowering developers to build and enhance ServiceNow solutions. It offers comprehensive documentation, training materials, code samples, and development tools. The 'Add to Update Set' utility, being a tool directly beneficial to ServiceNow developers during implementation and customization processes, logically resides on this site.

The ServiceNow Store, on the other hand, typically offers fully developed and supported applications, integrations, and services designed for a wider audience, not necessarily focused on core development utilities. The ServiceNow Community is a platform for user discussions, knowledge sharing, and problem-solving, while HI Support is primarily for incident resolution and technical assistance. While information about the 'Add to Update Set' utility might be found in the Community or addressed through HI Support if issues arise, the primary distribution point for the actual tool is the Developer site. Therefore, locating a developer-centric tool on the developer portal is the most appropriate place, aligning with the responsibilities of a Certified Implementation Specialist. The Developer Site is the one-stop-shop for the latest developer

resources.

Authoritative Link: developer.servicenow.com (Navigate to the tools or resources section to potentially locate the utility or related documentation).

Question: 36

What are the four values leveraged for the Inherent and Residual Risk Score Types?

A.Impact, Probability, SLE, ARO
B.Impact, Likelihood, SLE, ALE
C.Impact, Likelihood, SLE, Score
D.Impact, Likelihood, SLE, ARO

Answer: D

Explanation:

The correct answer is D: Impact, Likelihood, SLE, and ARO. These four values are fundamental in determining both the Inherent and Residual Risk Scores within ServiceNow's Risk and Compliance module. Let's break down why:

Impact: This represents the magnitude of the potential negative consequences if the risk materializes. A high impact signifies severe repercussions for the organization. Inherent and Residual risk scores consider the different level of impact on business functions.

Likelihood: This refers to the probability or chance of the risk actually occurring. A high likelihood indicates a greater chance of the risk becoming a reality. The risk of occurrence of a particular risk can affect the inherent and residual risk scores in terms of the level of vulnerability to an organization.

SLE (Single Loss Expectancy): This metric quantifies the expected financial loss from a single occurrence of the risk event. It is calculated by multiplying the Asset Value (AV) by the Exposure Factor (EF). This is crucial for prioritizing risks based on potential monetary damage. SLE is not commonly a key value to calculate Risk Scores.

ARO (Annualized Rate of Occurrence): This represents the estimated number of times a risk event is expected to occur in a year. It is used in conjunction with SLE to calculate the ALE (Annualized Loss Expectancy), which gives a comprehensive view of the expected financial loss due to the risk over a year. The ARO value allows you to calculate the financial impact of the risk as part of risk calculation.

The other options are incorrect because:

A, B, and C include "Score" or "ALEC," which are not standard values used directly in the inherent and residual risk score calculations themselves. While ALEC (Annualized Loss Expectancy Cost) is a derived value, the fundamental inputs are Impact, Likelihood, SLE and ARO.

In summary, ServiceNow leverages Impact, Likelihood, SLE, and ARO to provide a structured and quantifiable approach to assessing and managing risks. This approach enables organizations to prioritize risks effectively, allocate resources appropriately, and ultimately reduce their overall risk exposure.

Resources for more information:

ServiceNow Risk Management Documentation: (Search the official ServiceNow documentation portal using the term "risk assessment")
NIST Risk Management Framework: https://csrc.nist.gov/projects/risk-management (Although not ServiceNow specific, this is the general framework that Risk calculations are often based on).

Question: 37

What would you leverage in order to provide users with an alternate user experience to view policies, create policy exceptions, and search for controls?

A.Help Desk Portal

B.Catalog Portal

C.Access Portal

D.Service Portal

Answer: D

Explanation:

The correct answer is D, Service Portal. The Service Portal in ServiceNow is a self-service application offering a user-friendly, customizable interface to access services, information, and support. Specifically, it allows organizations to create a centralized location for users to interact with Risk and Compliance functionalities. Leveraging the Service Portal provides an intuitive alternative to the standard ServiceNow interface for tasks such as viewing policies (knowledge base integration), creating policy exceptions (request forms), and searching for controls (faceted search capabilities). The Service Portal offers greater flexibility in tailoring the user experience to specific needs and roles. Other portals are less suitable: the Help Desk portal focuses mainly on IT support requests, the Catalog portal centers on ordering services, and the Access portal manages user access requests. The Service Portal's versatility and customization options make it the ideal choice for presenting a dedicated risk and compliance experience. This streamlines user interaction, promoting wider adoption and adherence to risk and compliance processes. By configuring widgets and knowledge bases within the service portal, the user can effortlessly search through policies, identify relevant controls, and initiate exemption requests. This enhanced user experience encourages compliance adherence and contributes to better risk management practices.

ServiceNow Service Portal DocumentationServiceNow Risk and Compliance Documentation

Question: 38

What type of customers may you encounter? (Choose three.)

A.Organization recently acquired and had some bad audit findings (using ServiceNow GRC to help restart their process)

B.Organization with little to nothing in place already (implementing one or more core ServiceNow GRC applications)

C.Organization undergoing a full GRC transformation (implementing all three core ServiceNow GRC applications at once or in a phased approach)

D.Organization implementing ServiceNow GRC to help ease their Customer Service organization (using other tools to manage other processes)

E.Organization implementing ServiceNow GRC to help ease their Help Desk organization (using other tools to manage other processes)

Answer: ABC

Explanation:

The correct answer is ABC because these represent common scenarios where organizations would seek to implement ServiceNow GRC.

A: An organization that recently underwent an acquisition and received unfavorable audit results is an ideal candidate for ServiceNow GRC. The platform can help them streamline their risk and compliance processes, addressing the audit findings and establishing a robust framework for future governance. ServiceNow GRC's risk assessment capabilities would be crucial in identifying and mitigating risks exposed during the audit.

B: Organizations with minimal or no existing GRC infrastructure are prime candidates for ServiceNow GRC implementation. Starting from scratch allows them to build a comprehensive and integrated GRC program based on ServiceNow's best practices. They can leverage ServiceNow's out-of-the-box workflows, policy management, and control framework capabilities to build their GRC foundation.

C: An organization undergoing a full GRC transformation represents another key customer type. This might involve implementing all three core ServiceNow GRC applications (Risk, Compliance, and Audit Management) either simultaneously or in phases. ServiceNow GRC enables a holistic and integrated approach to GRC across the enterprise.

D and E are incorrect because ServiceNow GRC primarily addresses risk, compliance, and audit functions. While ServiceNow can integrate with Customer Service and Help Desk applications, the core value proposition of GRC lies in managing organizational risks, maintaining compliance, and facilitating audits, not easing the burden on those teams directly. While those teams might benefit indirectly, it's not the primary driver for a GRC implementation.

In summary, the scenarios in A, B, and C align with the target audience and typical use cases for ServiceNow GRC, focusing on organizations seeking to improve their risk management, compliance adherence, and audit readiness.

Here are some authoritative links for further research:

ServiceNow GRC Product Page:https://www.servicenow.com/products/grc.html
ServiceNow Risk Management:https://www.servicenow.com/products/risk-management.html
ServiceNow Compliance Management:https://www.servicenow.com/products/compliance-management.html

Question: 39

Possible regulations when Entity scoping for Healthcare:
(Choose two.)

A.HITRUST
B.FISMA
C.HIPAA
D.HETRUST

Answer: AC

Explanation:

The correct answer is A and C.

Justification:

When scoping entities within a healthcare organization for ServiceNow's Risk and Compliance module, it's crucial to consider applicable regulations. The Health Insurance Portability and Accountability Act (HIPAA) is a paramount US law that mandates the protection of sensitive patient health information (PHI). Entity scoping must include processes and systems that handle PHI to ensure compliance with HIPAA's privacy, security, and breach notification rules. This involves identifying specific departments, applications, databases, and

infrastructure components that are subject to HIPAA regulations.

The HITRUST Common Security Framework (CSF) is another significant standard within the healthcare industry. While not a law itself, HITRUST provides a comprehensive and prescriptive framework that incorporates various regulatory requirements, including HIPAA, into a single, certifiable framework. Many healthcare organizations and their business associates adopt HITRUST to demonstrate a robust security posture and compliance with industry best practices. Entity scoping should encompass elements that are part of the HITRUST CSF's scope for certification, ensuring that controls are appropriately mapped and assessed.

While FISMA (Federal Information Security Modernization Act) is important for federal information systems and agencies, it's not directly applicable to private sector healthcare organizations unless they are handling data on behalf of the federal government. HETRUST is not a known or recognized framework or regulation related to Healthcare compliance and Security.

Therefore, HITRUST and HIPAA are the two most relevant regulations when entity scoping for healthcare within ServiceNow's Risk and Compliance module.

Authoritative Links:

HIPAA:https://www.hhs.gov/hipaa/index.html
HITRUST:https://hitrust.com/

Question: 40

For Control records, who can modify the Control in the Draft state?

A.All compliance users
B.Only the Compliance Manager
C.Only the person assigned the Attestation
D.Only Control Owners

Answer: A

Explanation:

The correct answer is **A. All compliance users**.

Here's a detailed justification:

In ServiceNow's Risk and Compliance module, the Draft state of a Control record signifies that the control is still under construction and refinement. The system is designed to encourage collaboration and input during this initial phase. Broad accessibility ensures that various perspectives are considered before the control is finalized.

Compliance users, by definition, are individuals within the organization who have been granted specific roles and permissions related to compliance activities. This typically encompasses roles such as Compliance Managers, Risk Managers, Auditors, and other personnel involved in governance, risk, and compliance (GRC) processes. The intent is to allow users involved in the compliance process to contribute to, or review the compliance information present on the control record in order to ensure proper and accurate controls are in place to be implemented.

Limiting modification to only the Compliance Manager, the assignee of the Attestation, or Control Owners would restrict the flow of information and potentially lead to incomplete or inaccurate control definitions. This would contradict the spirit of collaboration and comprehensive risk management that ServiceNow aims to facilitate. The Compliance user role generally grants the necessary permissions to edit and contribute to

control records in the draft state. The other options are too restrictive. The system design is built in this fashion to reduce silos and encourage information sharing.

[ServiceNow Documentation on Roles and Permissions]: (Refer to official ServiceNow documentation for the specific roles and permissions associated with the Risk and Compliance module)(e.g., search for "ServiceNow GRC roles" or "ServiceNow Risk and Compliance permissions")[ServiceNow Community Forums]: (Search the ServiceNow Community for discussions on Control record workflows and user roles)(e.g., search for "ServiceNow Control record draft state permissions")

Question: 41

Control indicators may be triggered or scheduled in which state?

A.Retired
B.Monitor
C.Review
D.Attest
E.Draft

Answer: B

Explanation:

The correct answer is **B. Monitor**.

Control indicators in ServiceNow's Risk and Compliance application are designed to provide real-time or near real-time insight into the effectiveness of controls. They serve as triggers for automated monitoring and can also be scheduled for periodic assessments. The "Monitor" state reflects the active phase where the control indicator is actively gathering data, executing scripts, or performing other tasks to assess control performance. Control indicators residing in this state are the ones that can be triggered (either automatically based on events or manually) or scheduled to run based on defined frequencies. This allows for proactive identification of control weaknesses or failures.

Retired controls are inactive and will not be triggered or scheduled. Review, Attest, and Draft states typically precede the monitoring phase and are more related to creating, approving, or acknowledging the control indicator itself. The monitoring state is when the indicators are actively evaluating if the control is operating effectively. Only when an indicator is in the "Monitor" state, can it be actively triggered or scheduled for running assessments. Therefore, "Monitor" is the most appropriate state for triggering or scheduling control indicators.

For more information, refer to the ServiceNow product documentation for Risk and Compliance. You can often find detailed explanations and examples in the official ServiceNow documentation portal.

Question: 42

Which role reviews the risk response and moves the Risk record into the Monitor state at the appropriate time?

A.Risk Manager
B.Risk User
C.Risk Reader
D.Risk Owner

Answer: A

Explanation:

The Risk Manager is the appropriate role for reviewing the risk response and transitioning a Risk record to the Monitor state. This stems from their overall responsibility for managing and overseeing the risk management process. The Risk Manager is charged with validating the effectiveness of risk responses that the Risk Owner implements.

Here's why the other options are less suitable:

Risk User: This role typically has basic access to view and interact with risk records but lacks the authority to make decisions on the risk lifecycle stage. Their involvement is mainly for awareness and contribution of information.

Risk Reader: This role has very limited read-only access to risk records, lacking any authority to influence the risk workflow or state.

Risk Owner: While the Risk Owner is responsible for implementing the risk response plan, their primary focus is on executing the planned activities. Reviewing the efficacy of the implementation and shifting the risk to the Monitor phase is the Risk Manager's higher-level responsibility. After the Owner implements the response, the Manager then assesses and agrees with the move to Monitor.

The Monitor state signifies that the risk response has been implemented, and ongoing observation is required to ensure its continued effectiveness and that the residual risk remains within acceptable levels. The Risk Manager's oversight ensures that this monitoring is initiated and managed appropriately. The Risk Manager has the best view of all current risks and impacts and can decide when the record should be moved to monitor status.

Therefore, the Risk Manager possesses the necessary authority and responsibility to critically assess the risk response, determine if it's sufficient, and then initiate the monitoring phase by moving the Risk record to the Monitor state.

For further research, refer to ServiceNow's official documentation on Risk Management and role-based access control:

ServiceNow Docs: https://docs.servicenow.com/ (Search for "Risk Management" and "Roles in Risk Management")

Question: 43

Entity scoping is used for what?

A.Make sure that all of your Entities have the right visibility
B.Create and assign controls to the correct users
C.Create, assign, and manage controls and risks across an enterprise
D.Scope out the different users and roles that have access to the platform

Answer: C

Explanation:

Entity scoping in ServiceNow GRC (Governance, Risk, and Compliance) is primarily used to **create, assign, and manage controls and risks across an enterprise**. This means that rather than applying a single, broad-brush approach to governance, risk, and compliance, entity scoping allows organizations to tailor their GRC

activities to specific parts of the business (entities).

Let's break down why the other options are less accurate:

A. Make sure that all of your Entities have the right visibility: While visibility is a benefit of using entity scoping, it is not the primary purpose. The main goal is not simply to ensure visibility, but to actively manage and mitigate risks and ensure compliance within each entity.

B. Create and assign controls to the correct users: Again, control assignment is a part of GRC, and entity scoping can influence who has access and responsibility for controls within a given scope. However, this does not capture the broad organizational benefit of scoping.

D. Scope out the different users and roles that have access to the platform: While user roles and access control are important aspects of ServiceNow administration, they are not the specific concern of entity scoping. Entity scoping's goal isn't to restrict ServiceNow access generally, it is to manage risk and compliance differently for different parts of the company.

Entity scoping allows for a decentralized GRC approach where each entity can manage its unique risks and compliance requirements. For example, the financial division of a company will likely have risks and compliance requirements which are distinct from the sales or manufacturing divisions. By applying entity scoping, you can create targeted controls and risk assessments for each of these divisions, leading to a more relevant and efficient GRC program overall. This also ensures that the people who are responsible for a given entity can create and assign controls to the appropriate users.

Therefore, the correct answer is **C. Create, assign, and manage controls and risks across an enterprise**.

Authoritative Link:

ServiceNow GRC Documentation

Question: 44

The SOX content pack includes a series of policies, control, risks. How are all of these components linked together?

A.Mapping File
B.Manually
C.Automatically
D.Batch import

Answer: C

Explanation:

The correct answer is **C. Automatically**.

Here's why: The ServiceNow GRC (Governance, Risk, and Compliance) module is designed to automatically link policies, controls, and risks when using content packs like the SOX (Sarbanes-Oxley) pack. These packs are pre-configured with relationships established between these GRC elements. This automation is a core feature of ServiceNow GRC, promoting efficiency and reducing manual effort in managing compliance activities.

When you implement the SOX content pack, ServiceNow uses pre-defined relationships within the pack's metadata to create links. Risks are associated with specific controls designed to mitigate them. Controls, in turn, are linked to policies that dictate the overall compliance requirements. This automated linkage provides a clear traceability from a high-level policy down to the specific controls and risks impacted.

These relationships are typically established based on the best practices and regulatory requirements embedded in the SOX framework itself. For example, a policy regarding financial reporting accuracy will automatically be connected to controls (e.g., segregation of duties, approval workflows) that address the risks (e.g., misstatements, fraud) associated with inaccurate reporting.

This automation significantly reduces the administrative burden of manually mapping these components, which would be time-consuming and error-prone. It ensures a consistent and reliable framework for compliance management. The benefit is a clear audit trail, improved risk visibility, and streamlined compliance reporting. You can easily navigate the relationships through the ServiceNow interface, seeing how each component contributes to the overall compliance posture.

While manual adjustments can be made to these automatically generated relationships, the initial linkage is inherent in the content pack's design. Mapping files might be part of the content pack to facilitate the automation, but the process is automatic, driven by the configuration of those files. A batch import process may be involved in initially loading the data, but the linking of the data is automatic.

Relevant Links:

ServiceNow GRC Overview: https://www.servicenow.com/products/governance-risk-compliance.html ServiceNow Documentation (search for "GRC Content Packs"): https://docs.servicenow.com/ (you'll need a ServiceNow instance or login to access specific documentation)

Question: 45

UCF has a collection of what? Select all UCF terms.
(Choose three.)

A.Control Indicators
B.Authority Documents
C.Policies
D.Citations
E.Controls

Answer: BDE

Explanation:

The correct answer is BDE (Authority Documents, Citations, Controls). Let's break down why:

The Unified Compliance Framework (UCF) is essentially a curated library designed to simplify compliance management. Its core function is to map common requirements across various regulations, standards, and internal policies.

Authority Documents: The UCF references Authority Documents (like laws, regulations, and standards). These are the source documents from which compliance obligations are derived. Think of them as the root of any compliance requirement.

Citations: The UCF breaks down these Authority Documents into smaller, manageable pieces through Citations. Citations are specific, actionable statements extracted from the Authority Documents. This allows for granular management of compliance requirements. These are the actual sections, clauses, or provisions within regulations and standards.

Controls: The UCF provides Controls that are the standardized, actionable statements that must be implemented to satisfy the Citations from Authority Documents. These are the safeguard, measures, or procedures that organizations put in place to meet their compliance obligations. Controls are linked to

specific citations, showing which regulatory requirements they address.

Therefore, the UCF is a collection of Authority Documents, Citations, and Controls that allows businesses to build a common compliance framework that helps comply with various laws, regulations, and standards.

Why the other options are incorrect:

Control Indicators: While controls are part of the UCF, Control Indicators are metrics used to assess the effectiveness of those controls, not a fundamental component collected by UCF itself. These are typically defined and managed by organizations using the UCF as a reference.

Policies: While internal policies are important for compliance, the UCF primarily focuses on external requirements (laws, regulations, and standards) as well as mapping internal Policies. It is the basis for Policy creation but not a fundamental component it collects.

Relevant links for further research:

Unified Compliance Framework (UCF): (https://www.unifiedcompliance.com/) - You can visit the Unified Compliance website to learn about their framework, services, and resources.

UCF Terms and Definitions: (https://www.unifiedcompliance.com/resources/ucf-terms-and-definitions/) - This should provide a list of definitions of common UCF terms.

Question: 46

As a customer reaches greater GRC maturity, what can we expect to see occurring across their organization? (Choose three.)

A.Single Risk and Control frameworks across enterprise available to all stakeholders

B.Reliance on spreadsheet management for risk reporting

C.Continuous real-time monitoring of control performance

D.Cross-functional process automation

E.Reactive strategies for GRC activities

Answer: ACD

Explanation:

The correct answer is ACD. Here's why:

A. Single Risk and Control frameworks across the enterprise available to all stakeholders: Increased GRC maturity implies a move away from fragmented, siloed risk and control frameworks. A unified framework provides a single source of truth, streamlining governance, risk management, and compliance activities across the organization. This central repository makes it easier to manage and understand the organization's risk posture, and promotes consistent application of controls.

C. Continuous real-time monitoring of control performance: A mature GRC program emphasizes proactive risk management. Continuous monitoring leverages automation and data analytics to provide real-time visibility into control effectiveness. This allows for early detection of control failures and timely remediation, reducing the likelihood and impact of incidents. Reactive approaches are less prevalent in mature GRC implementations, which favor proactive approaches.

D. Cross-functional process automation: As organizations mature in GRC, they implement technologies to automate repetitive tasks, integrate workflows across departments, and enhance efficiency. This cross-functional automation eliminates manual processes, reduces errors, and improves auditability. It also enables better collaboration and communication between different teams involved in GRC activities.

Option B is incorrect because spreadsheet management is characteristic of immature GRC programs that rely on manual processes and have poor data visibility. Option E is incorrect because a mature GRC program focuses on proactive strategies.

Authoritative Links for further research:

ServiceNow GRC Solution: https://www.servicenow.com/products/governance-risk-compliance.html NIST Risk Management Framework: https://csrc.nist.gov/projects/risk-management

Question: 47

Which scheduled jobs in the GRC: Profiles scope help manage the population of Entity records? (Choose two.)

A.GRC indicator nightly run
B.GRC Entity and Risk Statement Data Collection
C.GRC Profile Generation
D.GRC Refresh Risk Scores

Answer: AC

Explanation:

The question asks about scheduled jobs within the "GRC: Profiles" scope that specifically aid in populating Entity records in ServiceNow. The correct answer is AC: GRC Profile Generation and GRC indicator nightly run.

Here's why:

A. GRC indicator nightly run: While not directly about profile creation, this scheduled job indirectly helps with the entity population. It does this by assessing indicators against defined thresholds, which in turn could trigger updates or creation of entities based on risk scores or assessment outcomes linked to those entities. This process maintains data integrity by reflecting the actual risk scores and assessment outcomes of entities in a timely manner.

C. GRC Profile Generation: This scheduled job directly drives the creation and/or updating of Entity Profiles based on pre-defined rules and criteria. When the job runs, it analyzes data within the system (e.g., configuration items, locations, departments, or users, depending on how GRC is configured) and generates/updates the corresponding entity profile records in ServiceNow. It uses profile types configured in the GRC module to perform the generation.

B. GRC Entity and Risk Statement Data Collection: This option primarily focuses on collecting risk statement data and doesn't contribute directly to the population of Entity records itself. It enriches entities with risk statements but doesn't create them.

D. GRC Refresh Risk Scores: The job focuses on updating risk scores of existing records and does not contribute to the creation of new Entity records.

Authoritative Links:

Unfortunately, direct, publicly accessible links describing the inner workings of specific ServiceNow scheduled jobs like "GRC Profile Generation" are scarce. ServiceNow documentation tends to be general.

However, one can understand the process of profile generation with GRC by reviewing the official documentation in the ServiceNow instance.

1. **ServiceNow Product Documentation:** While the documentation may not have detailed step-by-step instructions, you can generally find information about scheduled jobs and how to interact with them

via the ServiceNow product documentation website.

2. **Now Learning (ServiceNow Training Platform):** ServiceNow provides training materials and courses on the Now Learning platform, which often delve deeper into the functionalities of GRC modules, including scheduled jobs and their impact on Entity records.

Question: 48

Which of the following is the correct statement about Risk Scoring formulas?

A.SLE × ARO = ALE
B.ALE × ARO = Compliance Score
C.ALE × ARO = SLE
D.Impact × Urgency = ALE

Answer: A

Explanation:

The correct answer is **A. SLE × ARO = ALE**. Here's why:

ALE (Annualized Loss Expectancy): This represents the expected monetary loss for an asset due to a risk over a one-year period. It's a crucial component in risk assessment and helps prioritize mitigation efforts.

SLE (Single Loss Expectancy): This is the expected financial loss each time a risk event occurs. It's calculated by multiplying the asset's value by the exposure factor (percentage of asset value lost).

ARO (Annualized Rate of Occurrence): This represents the estimated number of times a risk event is expected to occur in a year.

The formula SLE × ARO = ALE is a standard method for calculating the ALE. It combines the potential loss from a single occurrence (SLE) with the likelihood of that occurrence happening within a year (ARO) to provide a comprehensive annual loss expectancy. This figure is vital for cost-benefit analysis when considering risk mitigation strategies. The other options are incorrect because they don't represent a standard risk calculation formula. Compliance Score isn't calculated this way, and the Impact x Urgency matrix typically contributes to qualitative risk assessments, not the precise financial calculation of ALE.

Supporting Resources:

1. NIST Special Publication 800-30, Guide for Conducting Risk Assessments: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/archive/2012-09-07
2. SANS Institute Reading Room: https://www.sans.org/reading-room/whitepapers/auditing/determining-risk-quantifying-annualized-loss-expectancy-1055

These resources provide detailed explanations of risk assessment methodologies, including the calculation of ALE and its importance in risk management. Understanding this formula is fundamental for anyone involved in risk and compliance, especially within the ServiceNow platform, as it helps in configuring and interpreting risk scoring models.

Question: 49

For classic risk assessment, while a Risk is in the Assess state, reviewers can do which of the following? (Choose two.)

A.Answer the assessment, moving the Risk to Respond

B.Set the Risk to Monitor

C.Delete the Risk

D.Set the Risk back to Draft

Answer: AD

Explanation:

The correct answer is A and D. Let's break down why:

A. Answer the assessment, moving the Risk to Respond: When a Risk is in the "Assess" state in ServiceNow's Risk and Compliance application, the core activity is to evaluate and quantify the risk. This involves responding to the assessment questions, providing details about the likelihood and impact of the risk. Completing the assessment and providing the necessary information is precisely what moves the risk to the next logical stage, which is "Respond." This stage deals with planning and implementing mitigation strategies based on the assessment results.

D. Set the Risk back to Draft: A reviewer might discover the Risk is not ready to be assessed or needs significant modifications, such as incorrect details or incomplete information. The reviewer can move the Risk back to the "Draft" state. Moving the risk back to the "Draft" state allows the risk owner to make the necessary changes or corrections before re-initiating the assessment process.

Why are B and C incorrect?

B. Set the Risk to Monitor: The "Monitor" state is usually associated with risks that have already been assessed, responded to (mitigated), and are now under observation to ensure the mitigation strategies are effective and the risk levels remain acceptable. Moving to "Monitor" before assessment would bypass the critical evaluation stage.

C. Delete the Risk: Deletion is a permanent action that's usually reserved for risks that are determined to be invalid or completely irrelevant. While possible depending on permissions, it's unlikely to be a standard activity performed during the Assess state, especially by reviewers. The appropriate course of action would typically be to set the risk back to Draft.

Justification using cloud computing concepts:

ServiceNow is a platform-as-a-service (PaaS) solution where risk management is orchestrated through a cloud-based application. The risk management lifecycle in ServiceNow is a structured workflow. The "Assess" state is a critical step in this lifecycle. The reviewers in this phase are responsible to answer questionnaires and provide the context to move the Risk to the Response Phase. ServiceNow provides capabilities to support these actions.

Authoritative Links:

ServiceNow Risk Management Documentation: (Access requires ServiceNow subscription or appropriate credentials). Search for "Risk Assessment Process" within the ServiceNow documentation portal.

ServiceNow Community Forums: (Requires ServiceNow account). Use the forums to search for discussions on Risk Assessment workflows and state transitions.

Question: 50

What is the condition that must exist to edit the factor guidance of a published risk assessment methodology (RAM)?

A.All assessment instance records are in the Monitor state

B.All assessment instance records are closed

C.All assessment instance records are deleted

D.States of the assessment instance records are irrelevant

E.All assessment instance records are canceled

Answer: C

Explanation:

The correct answer is C: All assessment instance records are deleted. Here's why:

Risk Assessment Methodologies (RAMs) in ServiceNow, once published and actively used, become templates for creating Risk Assessment instances. Editing the factor guidance directly affects how future risk assessments are conducted. To ensure data integrity and prevent inconsistencies, ServiceNow restricts modifications to the RAM when active assessment instances exist.

If assessment instances still exist, they rely on the current factor guidance for their evaluations. Altering the guidance mid-assessment could lead to inaccurate and misleading risk scores, potentially compromising compliance efforts. Therefore, a safeguard is in place.

Specifically, before the factor guidance can be edited, all risk assessment instances using that methodology must be deleted. Closing, canceling, or simply having them in a monitoring state doesn't suffice, because the historical link and dependence on the original guidance still exist. Deleting the instances breaks this dependency, allowing modification of the RAM without impacting active or past assessments. This restriction prevents changes to the methodology from retroactively affecting completed or in-progress risk
assessments, maintaining auditability and consistency. Deleting existing assessment instances effectively resets the link between the RAM and risk assessments, allowing for safe modification. Only after all links are broken can the underlying RAM be safely modified.

Refer to the ServiceNow documentation on Risk Management and Risk Assessment Methodologies for further details on these concepts and their implementation within the ServiceNow platform. The documentation specifically outlines the lifecycle of RAMs and the restrictions surrounding their modification.

Question: 51

Policies can be automatically published after which of the following occurs?

A.Related control objectives are marked active

B.Policy exception is closed

C.Policy is approved by all approvers

D.Policy is approved by one approver

Answer: C

Explanation:

The correct answer is C: Policy is approved by all approvers. Here's a detailed justification:

In ServiceNow's Risk and Compliance application, policies are not automatically published simply because related control objectives are active or a policy exception is closed. While these events might influence the policy lifecycle, they don't trigger automatic publication. Similarly, approval by a single approver is insufficient to guarantee the policy's overall validity and acceptance within the organization.

Automatic publishing of a policy typically occurs after a formal approval process involving all designated approvers. This is because policies often require sign-off from various stakeholders, including legal,

compliance, security, and business unit leaders, ensuring comprehensive review and organizational alignment. Once the policy passes through all approval stages defined in its workflow, the system can be configured to automatically publish it, making it accessible to the intended audience and setting it into effect. This ensures that the policy has been vetted appropriately before being put into action. The policy's "Approved" state signifies it has successfully navigated all predefined gates in the workflow.

The automated publication feature is commonly configured within the workflow or a business rule associated with the Policy table in ServiceNow. This automation streamlines the process, reduces manual effort, and ensures timely communication of policies across the organization. This approach minimizes the risk of policies being prematurely implemented or overlooked by critical stakeholders. The approval process acts as a control, verifying the policy's completeness and acceptability prior to its release.

While ServiceNow's documentation doesn't specifically address the precise trigger for automatic policy publication, the principle of requiring full approval before policy enforcement is widely understood within governance, risk, and compliance (GRC) frameworks. You can find general information about the policy and compliance module functionality here:

ServiceNow Risk Management: https://www.servicenow.com/products/risk-management.html
ServiceNow Compliance Management: https://www.servicenow.com/products/compliance.html (While a direct URL outlining the precise configuration details for automatic publishing based on approvals isn't publicly available without ServiceNow instance access, the general principles of workflow-driven automation in ServiceNow support this explanation.)

Question: 52

To allow other applications to request a policy exception, you must complete the integration registry form. In addition to providing the name of the registry entry, what additional information is needed to complete the form?

A.You must indicate the audience for requesting policy exceptions
B.You must indicate the intended Service Portal
C.You must indicate the policy exception target table
D.You must indicate the allowed policy acknowledgement campaigns

Answer: C

Explanation:

The correct answer is C: You must indicate the policy exception target table. This is because integrating with other applications to request policy exceptions inherently requires specifying where the exception requests will be stored and processed. The "policy exception target table" defines this destination within the ServiceNow Risk and Compliance application. This target table is the crucial link that allows external applications to interact with the policy exception workflow in a structured and predictable manner. Without specifying the target table, the ServiceNow instance won't know where to create the exception record, making the integration useless. The integration registry entry needs to establish the connection of where an inbound request creates the record.

Options A, B, and D are incorrect because they address aspects that are either managed elsewhere in the ServiceNow platform or are not fundamental for the initial integration setup. The audience of the exception request is often dictated by the integration and the application making the request and potentially managed via other system policies or access controls. Intended Service Portal is relevant for user interface
considerations but not for the core integration of request initiation, and policy acknowledgment campaigns focus on the validation of end users reviewing, understanding, and acceptance of the governance documents.

Therefore, the policy exception target table is essential for routing the exception requests correctly within

ServiceNow, making it the critical piece of information to configure in the integration registry form.

Further research on ServiceNow integration registries can be found at:

ServiceNow Documentation - Search for "Integration Registry" or "Table API"
ServiceNow Community - Look for articles and discussions on integrating with Risk and Compliance.

Question: 53

The overall goal of Entity Classes is to:

A.To enable reporting and to support advanced risk assessment
B.Show relationships between Entities and policies and map them directly to Citations
C.Associate Control Objectives and Risk Statements with Risks and Controls
D.To provide specific information about an Entity, such as who owns the Entity

Answer: D

Explanation:

The consensus answer, supported by a significant majority, suggests the overall goal of Entity Classes is to provide specific information about an Entity, such as who owns the Entity. While options A, B, and C touch upon aspects related to entities and their relationships within a GRC framework, they don't represent the primary goal of defining Entity Classes. Entity Classes fundamentally categorize and define the types of entities being managed within the GRC system. This classification allows for structured data input and consistent information capture about different types of business units, IT systems, or legal entities. Option D directly addresses this core function.

Think of Entity Classes as templates or blueprints for defining specific types of Entities. For example, an Entity Class could be "Data Center," which would then define the attributes and ownership information relevant to all Data Center Entities. This is crucial for consistent data management and accurate reporting. While reporting (A) is a downstream benefit, and relating Entities to policies/citations (B) and risks/controls (C) are subsequent actions, the foundation is accurate Entity definition (D). The owner of an Entity is a critical piece of identifying accountability and responsibility.

Therefore, option D is the most accurate representation of the primary purpose of Entity Classes. This foundational understanding then enables the other capabilities mentioned in the other options. Options A, B, and C are functionalities that can be leveraged after the Entities have been properly defined using Entity Classes.

Further research can be conducted through ServiceNow's official documentation regarding Entity Classes and their implementation within the Risk and Compliance module. Look for information on Entity Class creation, attribute definition, and their role in Entity management. While direct, publicly available links detailing this specific aspect can be limited, searching ServiceNow's knowledge base and community forums using terms like "ServiceNow GRC Entity Class definition," "ServiceNow Risk Management Entity ownership," or "ServiceNow Entity Class best practices" will yield helpful resources.

Question: 54

What is the minimum role required for creating a policy acknowledgement campaign?

A.sn_risk.user

B.sn_compliance.user
C.sn_compliance.admin
D.sn_compliance.manager
E.sn_control.owner

Answer: B

Explanation:

The correct answer is B, sn_compliance.user.

Creating a policy acknowledgment campaign in ServiceNow's Risk and Compliance application involves actions related to managing compliance policies and ensuring users acknowledge their understanding. The sn_compliance.user role grants the basic permissions needed to interact with compliance records, including policies and acknowledgments. It allows users to create and manage campaigns, define the target audience (users or groups required to acknowledge the policy), and track the acknowledgment status. While sn_compliance.admin and sn_compliance.manager certainly possess sufficient permissions, they are not minimally required. The sn_compliance.user role is specifically designed to allow general compliance team members to participate in policy acknowledgment workflows. sn_risk.user focuses on risk management activities, which are distinct from policy acknowledgment campaigns, even though both contribute to overall governance. sn_control.owner is related to the control framework, an entity separate from acknowledgement campaigns. Therefore, the role closest aligned with creating basic acknowledgement campaigns is the standard compliance user role.

For further research, explore the ServiceNow documentation on User Roles in Compliance and Risk Management:

ServiceNow Docs: https://docs.servicenow.com/ (Search for "compliance roles" or "risk management roles")
ServiceNow Community: https://community.servicenow.com/

Question: 55

Which of the following are the classic risk score types that ServiceNow tracks? (Choose three.)

A.Residual
B.Inherent
C.Calculated
D.Operational
E.Digital

Answer: ABC

Explanation:

The correct answer identifies the three classic risk score types tracked in ServiceNow Risk Management: Inherent, Residual, and Calculated.

Inherent Risk: This represents the risk level before any controls are implemented. It's the raw risk exposure based on the nature of the activity or process.

Residual Risk: This is the risk level after controls have been implemented. It represents the remaining risk exposure after considering the effectiveness of the controls in place. It’s calculated by subtracting the impact of mitigating controls from the inherent risk.

Calculated Risk: This score is automatically calculated based on the Inherent and Residual scores. The specific formula used is configurable, but it generally represents an aggregate view of the risk, considering both the initial exposure and the effectiveness of risk mitigation efforts. ServiceNow's architecture is specifically designed to automate risk calculation and tracking using these fundamental scores.

Operational risk (D) and Digital risk (E) are risk categories or areas, not fundamental risk score types. While ServiceNow can manage operational and digital risks, the system tracks them using the underlying Inherent, Residual, and Calculated scoring mechanism.

In essence, Inherent and Residual risk provide the building blocks while Calculated Risk gives an overall view of the risk landscape, allowing ServiceNow to effectively track and manage risks within an organization. The system provides features and functionalities to define, assess, and manage risks based on these scores, facilitating risk reporting and mitigation.

Refer to the following for additional information:

ServiceNow Risk Management documentation: (Requires ServiceNow instance access; specific document names may vary, search for "Risk Assessments" and "Risk Scoring".)
ServiceNow Community articles on risk management (requires ServiceNow Community login): (Search for related topics like "inherent vs residual risk" or "risk calculation methods").

Question: 56

What is the condition that must exist to edit the risk scoring logic of a published risk assessment methodology (RAM)?

A.All assessment instance records are closed
B.All assessment instance records are deleted or canceled
C.All assessment instance records are in the Monitor state
D.All assessment instance records are in the Draft state

Answer: B

Explanation:

The correct answer is **B. All assessment instance records are deleted or canceled.**

A published Risk Assessment Methodology (RAM) is a finalized template used for consistently evaluating risks. Modifying the risk scoring logic of a published RAM directly impacts past and future risk assessments using that methodology. ServiceNow prevents modification while active assessments exist to maintain data integrity and prevent inconsistencies in risk scoring across existing instances.

If assessment instance records based on the RAM are still active (in Draft, Monitor, or even Closed states), changing the scoring logic would retroactively alter the scores in those records, potentially leading to inaccurate risk profiles and flawed reporting. This retroactive change could violate audit trails and compromise the reliability of risk management data. Imagine suddenly changing the criteria after you've already graded a set of exams – the previous grades become invalid.

Therefore, before editing the risk scoring logic, all assessment instance records related to that RAM must be either deleted or canceled. Deletion removes the records entirely. Cancellation effectively archives the records, preventing further modification and excluding them from ongoing risk assessments. This action ensures that any changes to the scoring logic will only apply to new assessments created after the modification, preserving the integrity of past assessments and avoiding the retroactive alteration of existing risk data. This principle aligns with best practices for data governance and version control in cloud-based risk management systems. The deletion or cancellation safeguards against the unintended consequences of

modifying a published and actively used methodology.

Furthermore, the ServiceNow documentation emphasizes that changes to the RAM should only occur when there are no active assessments based on it.

Authoritative Links:

ServiceNow Documentation on Risk Assessment Methodologies: Search ServiceNow docs for "Risk Assessment Methodology" (Direct link cannot be provided as ServiceNow documentation requires authentication and changes frequently.) Look for information regarding the lifecycle of RAM and its impact on assessment instances.

Question: 57

Which of the following extends from Document Table? (Choose two.)

A.Citation
B.Policy
C.Control Objective
D.Authority Document

Answer: BD

Explanation:

The correct answer is B. Policy and D. Authority Document because both directly inherit from the Document table in ServiceNow. The Document table serves as a base table providing common fields and functionality for document-centric records within the platform. Policies and Authority Documents, which are key elements in Risk and Compliance, are naturally treated as documents, requiring features such as version control, attachments, and workflow capabilities provided by the Document table.

Citation (A) is typically related to instances of exceptions or violations of policy and would likely extend from a different base table, perhaps Task or a compliance-specific table that allows tracking of non-compliance issues. Control Objective (C) represents specific goals related to risk mitigation and may extend from a different base table like Configuration Item or a table better suited for defining targets and assessing effectiveness rather than being a general document.

Inheritance from the Document table allows Policies and Authority Documents to leverage existing functionalities within ServiceNow, ensuring consistency and ease of management. This design pattern minimizes redundancy and maximizes the benefits of a centralized document management system. The fields available on the Document table (e.g., number, state, created, updated, sys_created_by, sys_updated_by, short_description) are relevant to policies and authority documents, demonstrating the suitability of the inheritance. The classification of policies and authority documents as types of documents within ServiceNow is logical given their nature.

For further research, consider exploring the ServiceNow product documentation on base tables, especially the Document table, as well as information on Risk and Compliance data model. Examining the ServiceNow community forums for discussions on implementing Risk and Compliance solutions can also provide valuable insights.

Authoritative Links:

ServiceNow Product Documentation: (Requires ServiceNow instance access) Search within your ServiceNow instance documentation for "Document table", "Policy", and "Authority Document".
ServiceNow Community:https://community.servicenow.com/