PassQueen
a.k.a dumpsqueen.com

Certified Implementation Specialist - Risk and Compliance

ServiceNow CIS-RCI

Version Demo

Total Demo Questions: 16

Total Premium Questions: 167

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Risk and Compliance Overview	28
Topic 2, Risk Management	70
Topic 3, Policy and Compliance Management	55
Topic 4, Audit Management	11
Topic 5, Mix Questions	3
Total	167

QUESTION NO: 1

Which GRC tables serve as primary parent tables for the GRC applications? (Choose three.)

A. Content

B. Item

C. Asset

D. Task

E. Document

ANSWER: A D E

Explanation:

Content, Task, and Document are the primary parent tables used in the ServiceNow GRC/Integrated Risk Management data model. These tables provide shared, extensible foundations for records used throughout GRC applications, allowing common fields, workflows, relationships, security behavior, and lifecycle processes to be consistently inherited by more specific GRC record types. Content supports structured governance material and the content hierarchy used for items such as authorities, citations, controls, and related compliance content. Task provides the common task-based framework for actionable GRC work, enabling assignment, state management, approvals, activity tracking, and other operational behaviors used by GRC processes. Document provides the foundation for managed governance documentation, including policy-related records and associated document lifecycle capabilities. Understanding these parent tables is important when configuring forms, extending tables, creating reports, or designing integrations, because inherited fields and behaviors originate at the appropriate parent level. ServiceNow documents the common GRC data model and the relationships among its shared tables in its Integrated Risk Management product documentation: ServiceNow GRC data model. For the broader product context and GRC application capabilities, see ServiceNow Integrated Risk Management.

QUESTION NO: 2

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: A C

Explanation:

The `sn_grc_content` table is the base content table used by Integrated Risk Management Policy and Compliance capabilities to store reusable governance content. `sn_compliance_citation` extends this content model because a citation represents source material from an authority document, such as a regulatory requirement or industry standard, that can be referenced when building and assessing compliance content. This inheritance allows citations to retain common content attributes and participate consistently in the Policy and Compliance content lifecycle.

`sn_compliance_policy_statement` also extends `sn_grc_content`. A policy statement is managed content that defines an organization's required direction or expectation and can be related to citations, controls, and policy documents. Extending the shared Content table provides the common structure needed to author, organize, publish, and reuse policy-and-compliance content across the application.

ServiceNow's Policy and Compliance documentation describes the application's use of reusable content, including policy statements and authority-document citations. See the ServiceNow Policy and Compliance documentation and the authority documents documentation.

QUESTION NO: 3

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: A B C

Explanation:

ServiceNow's classic risk-scoring model tracks inherent, residual, and calculated risk scores. **Inherent** risk represents the level of risk that exists before controls and other mitigating measures are considered. It establishes the baseline exposure associated with the risk. **Residual** risk represents the exposure that remains after applicable controls are evaluated and their effectiveness is taken into account. This score helps risk owners and stakeholders understand whether the remaining exposure is within the organization's risk appetite or needs further treatment. **Calculated** risk is the system-derived score produced from configured scoring logic, such as likelihood and impact values, weighting, and other assessment inputs. It supports consistent, repeatable scoring across risk records and assessments. Together, these classic score types allow ServiceNow Integrated Risk Management to document the risk before mitigation, evaluate the remaining risk after mitigation, and maintain a calculated score based on the organization's defined methodology. ServiceNow's risk-management documentation describes risk records, assessments, and the scoring mechanisms used to support risk identification, analysis, and response. See the ServiceNow Risk Management documentation and the ServiceNow Integrated Risk Management product overview.

QUESTION NO: 4

Which of the following are a part of the GRC: Advanced Risk scope? (Choose two.)

A. Risk Hierarchy

B. Risk Assessment Methodologies

C. Risk Criteria Matrix

D. Risk Framework

ANSWER: A B

Explanation:

Risk Hierarchy and **Risk Assessment Methodologies** are components of the GRC: Advanced Risk application scope. The risk hierarchy provides the structured, parent-and-child organization of risks, allowing an organization to model risk relationships at different levels of detail. This structure supports consistent aggregation, reporting, ownership, and analysis of risks across the enterprise.

Risk assessment methodologies define the approach used to assess risks. They provide the assessment configuration and scoring logic needed to evaluate inherent and residual risk in a consistent, repeatable way. By using defined methodologies, organizations can align risk evaluations with their governance model and apply the appropriate assessment process to the relevant risks. Together, these Advanced Risk capabilities support a standardized risk-management lifecycle: organizing risks through the hierarchy and evaluating them through configured methodologies. ServiceNow describes Integrated Risk Management as connecting risk activities, processes, and data to enable informed decisions, while its product documentation provides the authoritative product guidance for configuring and using Risk Management features. See ServiceNow Integrated Risk Management and ServiceNow Product Documentation.

QUESTION NO: 5

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:

Tablename.LIST is the correct filter navigator syntax for opening a specified table's list view in a separate browser tab. In ServiceNow's application navigator, the table name is replaced with the actual database table name, such as `incident` or `sys_user`. Entering a value such as `incident.LIST` instructs the platform to navigate directly to that table's list while using the uppercase `LIST` suffix to open the result separately. This is useful for administrators and implementers who need to keep their current workspace or module context available while inspecting records in another table.

The behavior is part of ServiceNow's direct table-navigation shortcuts in the filter navigator. These shortcuts provide a fast alternative to expanding application menus and locating modules manually, particularly when working with system tables or performing configuration and validation tasks. ServiceNow documents the available direct-navigation formats, including the convention for opening a table list in a new tab, in its platform user-interface documentation: Navigate directly to a table.

QUESTION NO: 6

What can assessors do when a risk is in the state of Assess on a classic risk assessment?

Choose 2 answers

A. set the risk to Monitor

B. Delete the ns <

C. Deactivate the risk

D. Answer the assessment

E. set the risk back to Draft

ANSWER: A D

Explanation:

When a classic risk assessment is in the *Assess* state, the assessor's work is centered on evaluating the risk and progressing it after the evaluation is complete. **Answer the assessment** is therefore an assessor action: the assessor opens the generated assessment, supplies responses to the assessment questions, and submits the evaluation. Those responses provide the basis for the inherent or residual risk calculation and for subsequent risk-treatment decisions.

set the risk to Monitor is also available to the assessor in this lifecycle state. Moving the risk to monitoring indicates that the assessment activity has been completed and that the risk should proceed into ongoing observation, including continued tracking of its profile and related indicators where configured. This supports the classic Risk Management workflow by separating the active assessment task from the continuing monitoring of an assessed risk.

ServiceNow's Risk Management documentation describes risk assessment and lifecycle activities within Integrated Risk Management. See the ServiceNow Risk Management documentation and the risk assessment task documentation for the relevant process context.

QUESTION NO: 7

Which role is not part of ServiceNow GRC?

A. Risk User

B. Risk Developer

C. Risk Manager

D. Risk Reader

ANSWER: B

Explanation:

Risk Developer is the correct choice because it is not an out-of-box role in the ServiceNow Governance, Risk, and Compliance application, now generally presented as Integrated Risk Management. ServiceNow provides risk personas through defined roles that control access to risk records, assessments, and related workflow activities. The standard risk roles include Risk User, Risk Manager, and Risk Reader, each intended to grant an appropriate level of access for participating in, managing, or viewing risk-management work.

Role-based access control is fundamental to ServiceNow: users receive capabilities through assigned roles, and administrators can supplement the standard model with custom roles if an organization has specialized requirements. However, a role named Risk Developer is not among the standard GRC/IRM risk roles. An implementation team could create a custom role with that name, but it would not be a delivered ServiceNow GRC role and would not represent a standard persona in the product's role model.

For current product documentation on Integrated Risk Management roles and access, see the ServiceNow IRM roles documentation and ServiceNow's platform roles documentation.

QUESTION NO: 8

Which results can be configured to create an Issue automatically? (Choose three.)

A. Control test result is Failed

B. Attestation result is Not Implemented

C. Indicator result is Failed or Not Passed

D. Policy is approved by all approvers

E. Risk is moved to the Monitor state

ANSWER: A B C

Explanation:

A failed control test, **an attestation result of Not Implemented**, and **an indicator result of Failed or Not Passed** can be configured as issue-creation triggers. These outcomes identify potential deficiencies that require formal ownership and remediation tracking. Automatic issue creation preserves the context of the originating assurance activity and reduces the risk that a known gap is not addressed.

Organizations should configure issue-creation criteria according to their governance model so that significant control and compliance failures are consistently routed through the Issue Management lifecycle. See the ServiceNow Integrated Risk Management overview.

QUESTION NO: 9

The content table (sn_grcs_content) is a parent table of:

A. sn_grc_profile

B. sn_risk_framework

C. sn_risk_definition

D. sn_risk_risk

ANSWER: C

Explanation:

`sn_risk_definition` is correct because a risk definition is a type of GRC content and its table extends the Content table, `sn_grcs_content`. This inheritance lets risk definitions use common content capabilities and fields while also storing risk-specific information, such as the risk statement and attributes used to define and assess an organizational risk. In the ServiceNow table hierarchy, a child table inherits the fields and platform behavior of its parent table; therefore, fields defined on `sn_grcs_content` are available to records in `sn_risk_definition`. This design supports consistent management of reusable GRC content across Integrated Risk Management applications while allowing the risk-management data model to add fields that are specific to risk definitions. Administrators can verify this relationship in an instance by opening the table definition for Risk Definition and reviewing its Extends table value, or by using the Tables module to inspect the hierarchy. ServiceNow's Integrated Risk Management documentation provides the product context for risk definitions and common GRC data, and the platform documentation describes table extension and inherited fields. See the ServiceNow Risk Management documentation and the ServiceNow table extension documentation.

QUESTION NO: 10

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: A B

Explanation:

`sn_grc.manager` is required to provide manager-level access across Integrated Risk Management capabilities that support audit work. Audit managers commonly need to work with related GRC records and processes, such as risks, controls, issues, entities, and assessments, rather than being limited solely to the Audit Management application. This role provides the broader GRC management permissions needed for that cross-functional work.

`sn_audit.user` supplies the foundational Audit Management access used to participate in and operate audit-process functions. It enables access to audit records and activities that an Audit Manager must manage, including the operational work performed within the audit lifecycle. Combined with the Audit Manager role already assigned, it ensures that the user has both the Audit Management access foundation and the wider GRC manager permissions necessary to manage audit-related GRC activities.

ServiceNow documents Audit Management as an Integrated Risk Management application with role-based access, and its role model is designed so that users receive permissions appropriate to their audit and related IRM responsibilities. See the ServiceNow Audit Management documentation and the Audit Management roles reference.

QUESTION NO: 11

What is the name of the field on the entity that will keep the entity owner in sync with the source record owner field?

A. Auto-update Admin

B. Auto-update Mgr

C. Auto-update owner

D. Auto-sync owner

ANSWER: C

Explanation:

Auto-update owner is the entity-field setting used to keep an entity's Owner value aligned with the owner on its associated source record. Entities in Integrated Risk Management can be derived from source records such as CMDB configuration items or organizational records. Enabling this setting instructs the platform to update the entity owner as ownership changes on that source, helping maintain a reliable assignment of accountability without requiring manual edits to each entity record. This is particularly valuable in risk and compliance implementations because ownership is used for governance activities, task routing, and identifying the accountable person for an entity. The setting applies specifically to the owner relationship, so it preserves ongoing synchronization between the entity and its source record rather than being a one-time population action. This behavior supports the broader IRM approach of using a connected entity model to provide consistent context for risks, controls, assessments, and compliance work. See ServiceNow's Integrated Risk Management product information and the official ServiceNow product documentation portal for release-specific Entity Management configuration documentation.

QUESTION NO: 12

What is the primary purpose of an Issue record in Integrated Risk Management?

A. To track and remediate an identified deficiency

B. To publish a new authority document

C. To replace a policy acknowledgement campaign

D. To establish an entity hierarchy

ANSWER: A

Explanation:

To track and remediate an identified deficiency is correct. An issue provides a governed record for a problem identified through assurance activities, such as a failed indicator, unsuccessful attestation, control test, audit activity, or other assessment process. It can capture ownership, root cause, remediation work, target dates, and the status of corrective actions.

Issue Management gives stakeholders visibility into whether identified deficiencies are being addressed and whether remediation is completed in a timely manner. See the ServiceNow product documentation portal and the ServiceNow Integrated Risk Management overview.

QUESTION NO: 13

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: C

Explanation:

The minimum role required to create a policy acknowledgement campaign is **sn_compliance.admin**. Policy acknowledgement campaigns are administrative Compliance activities used to distribute published policy content to defined audiences, track acknowledgement responses, set campaign dates, and manage the campaign lifecycle. Creating such a campaign requires the elevated Compliance administration permissions supplied by this role. These permissions support configuration and management of Compliance application records, including the campaign setup needed to assign policy acknowledgements to users or groups and monitor their completion status.

Policy acknowledgement campaigns are part of ServiceNow Integrated Risk Management's Policy and Compliance capabilities. They provide an auditable mechanism for demonstrating that personnel have been asked to review and acknowledge organizational policies. Granting the administrative Compliance role to the campaign creator ensures that campaign definition, recipient targeting, notification behavior, and compliance reporting are managed by an authorized application administrator. For product and documentation resources, see the ServiceNow product documentation portal and the ServiceNow Integrated Risk Management overview.

QUESTION NO: 14

What dependency modeling feature can be used in the Classic UI to build relationships between Entity Classes?

A. GRC Workbench

B. Dependency Model Builder

C. Data Model Designer

D. GRC Tree Map

ANSWER: C

Explanation:

Data Model Designer is the Classic UI feature used to create and maintain relationships between Entity Classes in the ServiceNow Integrated Risk Management entity model. Entity Classes define the types of records an organization uses to represent its operational and risk-related landscape, such as business entities, processes, applications, and services. The designer provides a visual way to model how those classes relate, helping administrators establish the dependency structure that supports risk identification, assessment, and rollup across connected entities.

Using Data Model Designer, an implementation team can configure the relationship definitions needed by the entity framework without manually building the model solely through individual table and relationship-record configuration. This makes it especially useful when establishing or revising the organization's entity taxonomy and its dependencies in the Classic UI. The resulting model provides the relationship context that IRM can use when associating risks and other records with the entities affected by those dependencies. ServiceNow documents the IRM entity model and its configuration capabilities in the Integrated Risk Management product documentation. Additional platform documentation is available through the ServiceNow documentation portal.

QUESTION NO: 15

Who should be directly involved in GRC implementations? (Choose four.)

A. Board of directors

B. Chief Executive

C. ServiceNow platform experts

D. Business Analyst

E. Risk and compliance experts

F. CMDB process owner

ANSWER: C D E F

Explanation:

ServiceNow platform experts, Business Analyst, risk and compliance experts, and the CMDB process owner should be directly involved because each contributes a necessary implementation capability. ServiceNow platform experts translate approved requirements into scalable platform configuration, security, integrations, workflow, and data-model decisions. The Business Analyst elicits requirements, documents process designs, aligns user stories to business outcomes, and supports acceptance criteria. Risk and compliance experts provide the subject-matter knowledge needed to ensure that risk taxonomies, control objectives, assessments, authority documents, and compliance processes accurately reflect the organization's GRC program. The CMDB process owner is particularly important when the implementation uses technology assets or configuration items as risk objects, control scope, evidence sources, or assessment targets; this role helps establish data ownership, quality, and appropriate CMDB integration. Together, these participants connect the GRC operating model, the detailed business processes, the platform's technical design, and the underlying configuration data needed for reliable reporting and automation. ServiceNow describes Integrated Risk Management as a connected approach to identifying, assessing, prioritizing, and monitoring risk, while CMDB guidance emphasizes managing configuration-item data used across the platform. See ServiceNow Integrated Risk Management and ServiceNow CMDB.

QUESTION NO: 16

What is the purpose of a policy acknowledgement campaign?

A. To request and track acknowledgement of published policy content

B. To create a new Authority Document

C. To calculate an annualized loss expectancy

D. To assign an Entity Class to a CMDB record

ANSWER: A

Explanation:

To request and track acknowledgement of published policy content is correct. A policy acknowledgement campaign distributes a published policy to a defined audience and records whether assigned users have acknowledged it. The campaign provides due dates, completion status, and reporting that help organizations demonstrate that personnel were requested to review applicable policy content.

Acknowledgement does not replace policy approval or publication. Instead, it is an awareness and attestation activity performed after the policy is available to its intended audience. See the ServiceNow Integrated Risk Management product overview and the ServiceNow product documentation portal.