PassQueen
a.k.a dumpsqueen.com

Certified Implementation Specialist -Vendor Risk Management

ServiceNow CIS-VRM

Version Demo

Total Demo Questions: 8

Total Premium Questions: 83

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Vendor Risk Management Overview	9
Topic 2, Vendor Risk Management Application Administration	27
Topic 3, Vendor Risk Management Implementation	9
Topic 4, Vendor Risk Assessment	22
Topic 5, Vendor Risk Issue Management	12
Topic 6, Vendor Risk Integrations	3
Topic 7, Mix Questions	1
Total	83

QUESTION NO: 1

A Vendor Risk Assessment that consists of a SIG Lite questionnaire and two document requests are displayed as how many total requests in the Vendor Portal?

A. 2

B. 3

C. 0

D. 1

ANSWER: B

Explanation:

3 is correct. In the Vendor Portal, the assessment work is presented to the vendor as distinct requests based on the assessment content that requires a response. The SIG Lite questionnaire is one request, because it is a questionnaire response task. Each of the two document requests is also presented as its own request so the vendor can upload the specified evidence or supporting documentation independently. Therefore, the vendor sees one questionnaire request plus two document requests, for a total of three requests. This separation helps vendors identify the action required for each item, enables documents to be collected and reviewed against their individual requirements, and allows the assessment owner to monitor completion of questionnaire and evidence-collection work. ServiceNow Vendor Risk Management supports assessing vendors through questionnaires and collecting supporting documentation as part of the vendor-assessment process. See the ServiceNow Vendor Risk Management product overview and the Vendor Risk Management documentation for product and process context.

QUESTION NO: 2

A Vendor Risk Task can be created from which of the following records?

A. Policy, Assessment, Vendor

B. Risk, Policy, Assessment

C. Policy, Vendor Risk issue, Assessment

D. Vendor Risk Issue, Assessment, Vendor

ANSWER: D

Explanation:

Vendor Risk Issue, Assessment, Vendor is correct. Vendor Risk Management uses Vendor Risk Tasks as actionable work items that can be initiated in the context of a vendor record, an assessment, or a vendor risk issue. Creating a task from a vendor supports work that applies broadly to the third-party relationship, such as obtaining supporting documentation or coordinating a vendor-contact follow-up. Creating one from an assessment ties the work to assessment activities and evidence collection. Creating one from a Vendor Risk Issue supports tracking and assigning remediation or issue-resolution activities. In each case, the originating record provides the task's business context, enables appropriate ownership and due-date management, and lets users follow task progress from the relevant vendor-risk workflow. This supports traceability between operational actions and the vendor, assessment, or issue that prompted the work. ServiceNow's Vendor Risk Management documentation describes VRM capabilities for assessing vendors, identifying and managing vendor risk issues, and tracking related remediation activities. See the ServiceNow Vendor Risk Management documentation and the Vendor Risk Management product overview.

QUESTION NO: 3

Which could have an impact on the vendor's Risk Assessment rating? (Choose three.)

A. Answering one or more questions incorrectly

B. Leaving answers blank

C. Omitting documentation

D. Spelling errors

E. Reassigning a questionnaire to a contact

ANSWER: A B C

Explanation:

Risk Assessment ratings in Vendor Risk Management are driven by the evaluation of questionnaire responses and supporting evidence against the assessment's configured scoring logic. **Answering one or more questions incorrectly** can directly change the calculated result because scored answers map to risk values, weights, or outcomes defined in the questionnaire and assessment methodology. **Leaving answers blank** can also affect the rating when unanswered items are treated as incomplete, receive a configured default score, or prevent the assessment from being fully evaluated. **Omitting documentation** affects the assessment when evidence is required to substantiate a response: the assessor may score the response based on the absence of evidence or identify a gap that contributes to the vendor's assessed risk. These factors concern the completeness, validity, and scoring of the vendor's submitted assessment data, which are the inputs used to determine a risk result. ServiceNow Vendor Risk Management supports questionnaire-based vendor assessments, evidence collection, and risk evaluation as part of the vendor-risk process. See the ServiceNow Vendor Risk Management documentation and the ServiceNow Vendor Risk Management product overview.

QUESTION NO: 4

What is the definition of â€˜Risk Managementâ€™?

A. Policies/Standards/Procedures established to ensure an organization is aligned with corporate strategy and expectations are clearly defined

B. The process of conforming to standards, policies, and remediation of audit findings

C. The elimination of vulnerable surface area in an enterprise environment

D. Process to identify, assess, and respond to risks, threats and vulnerabilities that could compromise the business

ANSWER: D

Explanation:

Process to identify, assess, and respond to risks, threats and vulnerabilities that could compromise the business is the correct definition of risk management. Risk management is a continuous business discipline for recognizing events or conditions that may affect objectives, analyzing their likelihood and potential impact, deciding how they should be treated, and tracking the treatment through completion. The response can include reducing the risk through controls, transferring it, accepting it within approved tolerance, or avoiding the activity that creates it. In a ServiceNow Integrated Risk Management implementation, this lifecycle supports a structured and traceable approach: risks can be recorded, evaluated against defined criteria, assigned to accountable owners, connected to controls or issues, and monitored as the organization's risk posture changes. This definition appropriately includes both the assessment stage and the action taken after assessment, rather than treating risk management as only policy creation or audit remediation. ServiceNow describes risk management as helping organizations identify, assess, prioritize, and respond to risks in a consistent way; see ServiceNow: What is risk management?. The same lifecycle aligns with the risk-management guidance in NIST's Risk Management Framework overview, which emphasizes assessing risk and authorizing or monitoring risk responses throughout an ongoing process.

QUESTION NO: 5

Which of the following is an objective of Vendor Risk Management? (Choose two.)

A. To help vendors improve their security posture and preparedness

B. To assess and manage the risk from interactions with vendors and third parties

C. To help negotiate the best possible price for a product or service from the vendor

D. To verify that vendors have adequate measures and processes in place to ensure profitability of vendor

ANSWER: A B

Explanation:

Vendor Risk Management is intended to provide a consistent, risk-based process for overseeing the organization's relationships with suppliers and other third parties. Therefore, **To assess and manage the risk from interactions with vendors and third parties** is a core objective. Teams use inherent-risk assessments, due diligence questionnaires, evidence collection, issue remediation, and ongoing monitoring to understand a vendor's potential effect on areas such as information security, privacy, operational resilience, and regulatory compliance. This allows the organization to make informed decisions before and throughout a vendor relationship.

To help vendors improve their security posture and preparedness is also an appropriate objective. Risk assessments can identify control gaps or unmet requirements, while remediation activities and corrective-action plans provide a structured path for vendors to address those gaps. Improving the vendor's relevant controls reduces residual risk for both the vendor and the customer organization, particularly where the vendor processes sensitive data or supports critical business services. ServiceNow describes its Vendor Risk Management capabilities as enabling organizations to assess, monitor, and manage third-party risk throughout the vendor lifecycle. See ServiceNow Vendor Risk Management and ServiceNow Integrated Risk Management.

QUESTION NO: 6

Key data sources for Vendor Risk reporting include which of the following tables? (Choose two.)

A. Vendor Risk Assessment [sn_vdr_risk_asmt_assessment]

B. Questionnaire Templates [asmt_metric_type]

C. Vendor Benchmark Scores [sn_vdr_client_score]

D. Survey Scores [snc_survey_scores]

E. Vendor Risk Issue [sn_vdr_risk_asmt_issue]

ANSWER: A E

Explanation:

Vendor Risk Assessment [sn_vdr_risk_asmt_assessment] and **Vendor Risk Issue [sn_vdr_risk_asmt_issue]** are key reporting data sources because they contain the operational records that describe a vendor's assessment activity and the issues identified through that activity. Assessment records provide the primary reporting population for tracking assessment status, progress, results, and vendor risk evaluation activity. They support reports and dashboards that need to show how assessments are distributed across vendors, where they are in the lifecycle, and the outcomes produced by the assessment process.

Issue records are equally important because they represent risk findings that require attention, remediation, exception handling, or ongoing monitoring. Reporting on these records enables risk teams to identify open issues, assess severity and ownership, monitor remediation progress, and understand the concentration of unresolved vendor-related risk. Together, the assessment and issue tables support the core Vendor Risk Management reporting flow: evaluate vendors through assessments, identify issues from findings, and track those issues to closure. This aligns with ServiceNow's Vendor Risk Management capabilities for continuous assessment and issue-driven risk oversight. See the ServiceNow Integrated Risk Management overview and the ServiceNow product documentation portal.

QUESTION NO: 7

In the Vendor Portal, who can reassign Assessments?

A. Vendor Business Owner

B. Vendor

C. Primary Contact

D. Vendor Manager

ANSWER: D

Explanation:

Vendor Manager is correct. In Vendor Risk Management, the Vendor Portal supports collaboration between an organization and its vendor contacts during assessment completion. The Vendor Manager is the vendor-side role intended to coordinate the vendor's assessment activity, including managing who is responsible for completing an assessment. This role can reassign an assessment to an appropriate vendor contact when the initially assigned person is unavailable, is not the subject-matter expert for the questions, or when responsibility changes. Reassignment helps ensure that the assessment is completed by the individual best positioned to provide accurate responses and supporting evidence, while allowing the vendor's work to continue without requiring the internal risk team to manually redirect every task. The Vendor Manager therefore acts as the vendor's operational coordinator in the portal, maintaining appropriate ownership of assessment work across the vendor's contacts. ServiceNow describes Vendor Risk Management as a workflow for assessing and monitoring third-party risk, with vendor engagement and assessment collection being core activities. See the ServiceNow Vendor Risk Management documentation and the ServiceNow Vendor Risk Management product overview.

QUESTION NO: 8

If clean data is not provided by the customer, what baseline solutions are available within the platform? (Choose three.)

A. Integration hub ETL plugin

B. Field normalization plugin

C. Service graph connector

D. System definition fix scripts module

E. System import transform map scripts

ANSWER: A B D

Explanation:

The baseline platform capabilities for addressing customer data that is incomplete, inconsistent, or not standardized are **Integration hub ETL plugin**, **Field normalization plugin**, and **System definition fix scripts module**. IntegrationHub ETL provides a guided, reusable approach for extracting, transforming, and loading data, enabling implementers to map source values into the structures required by the ServiceNow application. This is particularly useful when data arrives from multiple systems or requires repeatable transformation during migration and ongoing imports. The Field Normalization capability supports consistent field values by applying normalization logic, reducing duplicates and variations in values that should represent the same business concept. Fix scripts provide a controlled mechanism to perform one-time, bulk corrective updates to existing records during implementation or remediation activities. Together, these capabilities support an implementation approach in which incoming data is transformed, values are standardized, and existing records can be repaired where necessary before the data is relied on for Vendor Risk Management processes and reporting. See ServiceNow's Integration Hub overview and the IntegrationHub ETL documentation.