Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.

KILL EXAMS

CIS-RC Practice Questions
CIS-RC Practice Test
CIS-RC Practice Exam
CIS-RC Exam Questions
CIS-RC Study Guide

PASS

killexams.com

ServiceNow

CIS-RC

ServiceNow Certified Implementation Specialist - Risk and Compliance (CIS-RC)

Question: 1441

Testing protocols in a publishing house's CIS-RC must simulate content risk escalations from AI-generated texts. Which protocols adapt?

A. AI-input fuzzing in ATF to test protocol responses to generative variances
B. Bias detection integrations in tests, validating protocol fairness metrics
C. Scenario-based evals with ethical AI frameworks, scoring protocol alignments
D. Iterative protocol tuning via ML feedback from test outcomes

Answer: A, C, D

Explanation: Fuzzing tests variances. Evals score ethics. Tuning refines via ML.

Question: 1442

What is a significant use of risk assessment templates in the context of vendor risk management?

A. Rapid deployment of vendor assessments consistent with organizational policies
B. Summarizing audit findings
C. Closing vendor accounts
D. Handling vendor payroll

Answer: A

Explanation: Templates streamline vendor risk evaluations ensuring assessments align with established policies and compliance requirements.

Question: 1443

Which type of indicator would you use in ServiceNow CCM if control data is collected manually from external systems where automated data retrieval is not possible?

A. Basic Indicator
B. Scripted Indicator
C. Manual Indicator
D. Automatic Indicator

Answer: C

Explanation: Manual Indicators are designed for cases where control data comes from outside ServiceNow or other manual sources, requiring assigned tasks to users to validate compliance manually.

Question: 1444

A non-profit organization scaling international aid programs identifies donor privacy risks in the identification phase of the Classic Risk Assessment Lifecycle. GDPR alignments are required. Which approaches support this? (Select all that apply)

A. Integrate with CRM systems to identify privacy gaps in donor data handling
B. Create GDPR-specific risk templates for standardized privacy threat documentation
C. Assign compliance roles during identification to oversee donor risk logging
D. Use reporting tools to analyze identified privacy risks for program impact

Answer: A, B

Explanation: Non-profit donor privacy identification needs CRM integrations and templates for GDPR adherence. CRM pulls reveal handling gaps, automating discovery. GDPR templates ensure standardized threat capture, fitting the phase. Role assignments and reporting are later-stage activities.

Question: 1445

In a tech startup scaling its operations globally, the GRC team is tasked with creating policy documents for AI ethics that include control statements mandating bias detection artifacts from ML models. To handle the complexity of maintaining these amid rapid iterations, which advanced practices should be adopted for control statements to integrate with DevOps pipelines and ensure artifact traceability in CI/CD environments?

A. Integrate control statements with IntegrationHub spokes for automated artifact pulls from Git repositories during policy maintenance
B. Define control statements with parameterized queries to dynamically reference versioned artifacts in DevOps tools like Jenkins
C. Enable audit trail extensions on related artifacts to log CI/CD pipeline interactions for compliance verification
D. Configure policy exception workflows to route control statement deviations detected in automated artifact scans

Answer: A, B, C

Explanation: IntegrationHub spokes allow control statements to pull artifacts directly from Git repositories, automating synchronization during policy maintenance and bridging GRC with DevOps for agile scaling. Parameterized queries in control statements dynamically reference versioned artifacts from tools like Jenkins, accommodating rapid iterations without static linkages that could break traceability. Audit trail extensions on artifacts capture CI/CD interactions, providing verifiable logs essential for

demonstrating ethical AI compliance in global expansions.

Question: 1446

For regulatory reporting use cases, what role does the Policy Library serve in ServiceNow GRC?

A. Scheduling audit meetings
B. Repository for compliance policies that govern reporting requirements
C. Vendor onboarding
D. Incident tracking

Answer: B

Explanation: The Policy Library stores all compliance and reporting policies, providing easy access and linkage to controls and reporting activities.

Question: 1447

A telecommunications provider is implementing GRC with emphasis on continuous control monitoring in the Xanadu release, but encounters bottlenecks in stakeholder alignment for performance analytics setup. Which implementation team roles should drive the resolution by linking analytics indicators to entity risk statements?

A. Performance analytics specialists configuring indicator sources
B. Project managers aligning stakeholders on KPI definitions
C. Risk and compliance experts validating linkages to risk statements
D. Technical implementers deploying data collectors for real-time feeds

Answer: B, C

Explanation: Resolving bottlenecks in performance analytics setup for continuous monitoring involves project managers aligning stakeholders on KPIs to ensure consensus. Risk and compliance experts validate that indicators accurately link to entity risk statements, supporting Xanadu's enhanced monitoring. Specialists and implementers execute configurations, not drive resolution.

Question: 1448

Which component in ServiceNow GRC manages the assignment and review of control activities?

A. Risk Registers
B. Policy Management
C. Control Testing and Assessment
D. Incident Management

Answer: C

Explanation: Control Testing and Assessment handles creating, assigning, and reviewing control activities to ensure that risk controls function as intended and are properly examined over time.

Question: 1449

In ServiceNow, what is the potential downside of assigning multiple overlapping roles directly to a single user?

A. Faster performance
B. Simplified audit trails
C. Increased risk of privilege escalation
D. Automatic role reconciliation

Answer: C

Explanation: Overlapping roles can aggregate excess permissions leading to privilege escalation, making it harder to enforce least privilege principles and increasing security risks.

Question: 1450

An aerospace firm's safety policies version attachments for flight simulation data with regulatory filings. Filing rejections cascade version invalidations. Which rejection handlers?

A. Auto-rollback workflows to prior valid versions on filing rejections
B. Rejection tagging in attachments for targeted re-versioning cycles
C. Lifecycle quarantine states isolating invalidated attachment versions
D. Predictive validation scripts pre-filing to minimize rejection cascades

Answer: A, C, D

Explanation: Rollback workflows revert to valid versions post-rejection, maintaining safety continuity. Quarantine states isolate issues, allowing parallel fixes. Predictive scripts validate upfront, reducing cascades in aerospace regulatory lifecycles.

Question: 1451

Which statement correctly describes the role of GRC in Integrated Risk Management (IRM)?

A. GRC only monitors financial risk

B. GRC forms a core component facilitating risk identification, assessment, and mitigation across business units
C. GRC is unrelated to risk but handles compliance only
D. IRM replaces GRC entirely

Answer: B

Explanation: GRC is a foundational component of IRM, providing processes and tools that allow organizations to identify, assess, manage, and mitigate risks holistically across the enterprise.

Question: 1452

During a merger integration, a tech conglomerate's RCM setup must handle cross-jurisdictional alerts from multiple feeds, including Regology for APAC regulations. To prevent compliance gaps, which extended capabilities in RCM should be leveraged for dynamic applicability determination and automated remediation planning?

A. Define custom taxonomy classes for merger-specific sectors to enhance feed auto-assignment and reduce false positives in alert generation.
B. Activate the Applicability Assessment workflow to evaluate alerts against entity classes, routing non-applicable ones to cancellation with rationale logging.
C. Integrate RCM with Operational Risk Management to auto-create risk events from high-applicability alerts, including scenario-based mitigation templates.
D. Configure the Change Implementation phase to generate branched action plans based on jurisdiction-specific control mappings.

Answer: B, C, D

Explanation: The Applicability Assessment workflow in RCM systematically evaluates alerts against predefined entity classes and profiles, automatically routing inapplicable ones to a canceled state while mandating rationale documentation to support audit defensibility and prevent oversight in complex merger scenarios. Integrating RCM with Operational Risk Management enables the creation of risk events from applicable alerts, incorporating scenario-based templates that align mitigations with organizational risk appetite and jurisdictional nuances. In the Change Implementation phase, RCM supports branched action plans derived from control mappings, ensuring remediation strategies are tailored to specific regulatory contexts and executed efficiently across global operations.

Question: 1453

A healthcare organization is implementing GRC with a focus on HIPAA compliance in the Xanadu release, where the implementation team discovers overlapping responsibilities in control objective assignments across entity types. In this scenario, who should lead the remediation effort to refine the entity architecture while incorporating performance analytics indicators for ongoing monitoring?

A. Internal audit experts reviewing control mappings for audit trail completeness

B. Project managers coordinating cross-functional reviews to update the implementation roadmap
C. Risk and compliance experts designing refined entity class hierarchies with analytics integration
D. Technical implementers deploying UI policies for entity type visibility restrictions

Answer: B, C

Explanation: In GRC implementations addressing overlapping responsibilities in entity architectures, particularly for regulated sectors like healthcare under HIPAA, project managers lead remediation by coordinating reviews and adjusting the roadmap to incorporate Xanadu-specific features like enhanced analytics. Risk and compliance experts are key in designing refined hierarchies for entity classes, ensuring control objectives align with performance indicators for real-time monitoring. Internal audit experts provide validation post-remediation, while technical implementers execute deployments rather than leading design efforts.

Question: 1454

In designing risk owner personas in ServiceNow, which approach best ensures granular access control while minimizing administrative overhead?

A. Assign individual user roles directly for all permissions
B. Assign roles manually to users without groups
C. Use only out-of-the-box roles without customization
D. Leverage group membership combined with role inheritance

Answer: D

Explanation: Leveraging group membership combined with role inheritance provides scalable and manageable access control. It groups users by function and assigns roles to the group rather than individuals, reducing manual role assignments and improving maintainability.

Question: 1455

In the context of regulatory reporting, what is a benefit of automated evidence collection?

A. Increases audit readiness by maintaining real-time compliance documentation
B. Slows down report generation
C. Removes audit requirements
D. Limits user participation

Answer: A

Explanation: Automation ensures relevant evidence is collected continuously, easing audit preparation and compliance verification.

Question: 1456

A creative agency managing client IP in virtual production environments must refine policy documents, where control statements link to AR/VR asset artifacts and rights clearance logs. Facing creative workflow complexities, which immersive tech adaptations for control statements facilitate artifact versioning in metaverse integrations?

A. Adapt control statements with 3D metadata extractors for AR/VR artifact versioning
B. Configure metaverse hooks to synchronize asset artifacts with policy control updates
C. Use collaborative VR sessions for joint control statement reviews with embedded artifacts
D. Implement watermarking protocols on artifacts to trace usage in virtual control validations

Answer: A, B, D

Explanation: 3D metadata extractors version AR/VR artifacts, aligning with control statements for IP management. Metaverse hooks synchronize updates, bridging virtual and policy realms. Watermarking traces artifact usage, bolstering control validations in creative flows.

Question: 1457

What does risk prioritization involve within ServiceNow's Risk Assessment?

A. Ranking risks based on combined impact and likelihood
B. Evaluating risks solely on probability
C. Assigning subjective importance to each risk
D. Ignoring low-scoring risks

Answer: A

Explanation: Prioritization considers both likelihood and impact to rank risks objectively, ensuring the highest threats receive attention first.

Question: 1458

Why is it important to maintain version history on control libraries?

A. To audit control changes and support compliance investigations
B. To speed up evidence collection
C. To automate policy creation
D. To assign control owners automatically

Answer: A

Explanation: Version histories provide a record of control evolution necessary for audit trails and regulatory inquiries.

Question: 1459

In advanced risk framework configurations, what feature supports multi-dimensional risk scoring?

A. Binary pass/fail criteria
B. Scorecard aggregation
C. Manual overrides only
D. Single attribute scoring

Answer: B

Explanation: Scorecard aggregation combines multiple attribute scores into a composite measure, enabling multi-dimensional risk evaluation.

Question: 1460

A banking institution post-data breach enhances its Classic Risk Assessment Lifecycle by focusing on fraud vector identification in payment systems. ServiceNow configurations must sync with fraud detection tools. Which practices ensure comprehensive identification? (Select all that apply)

A. Configure fraud pattern matching in risk statements for automated vector logging
B. Integrate with SIEM systems to pull anomaly data into risk identification records
C. Deploy dashboards for ongoing identification monitoring of payment fraud trends
D. Enforce risk owner assignment immediately upon identification for accountability

Answer: A, B

Explanation: Banking fraud identification demands pattern-based statements and SIEM integrations to document vectors thoroughly, aligning with the phase's exploratory goals. Fraud pattern matching in statements automates logging of common threats, enhancing precision in payment ecosystems. SIEM integrations import anomaly insights directly, bolstering discovery without manual intervention. Dashboards suit monitoring, and immediate assignments are response-oriented.

Question: 1461

Which of these is a ServiceNow best practice for managing personas in large organizations?

A. Assign roles individually to every user
B. Bypass role assignments for speed
C. Use groups and role inheritance to manage access
D. Utilize only admin roles

Answer: C

Explanation: Using groups with role inheritance simplifies administration, ensures consistency, and provides scalable access control in large deployments.

Question: 1462

In a supply chain platform, custom GraphQL integrations pull blockchain-verified vendor data into GRC. For traceability in compliance audits, which capabilities enhance the integration?

A. Define GraphQL schemas in GRC to query blockchain nodes for immutable vendor evidence.
B. Configure resolvers in Integration Hub to validate data against GRC control assertions.
C. Enable caching layers for frequent queries to optimize performance during audits.
D. Integrate with GRC Analytics to visualize blockchain-sourced risk chains.

Answer: A, B, D

Explanation: GraphQL schemas allow direct querying of blockchain for evidence, ensuring immutability in GRC. Resolvers validate against controls, maintaining data integrity. Analytics visualizations map risk chains, aiding audit transparency in supply chains.

Question: 1463

In a defense contractor's GRC setup, classified entity scopes require air-gapped integration with ITSM's Vulnerability Response for control patching. The data model's domain partitioning in Xanadu release is key. Which architectural features support this secure integration, maintaining data isolation while enabling vulnerability-risk correlations?

A. Domain-separated Vulnerability groups mapped to GRC Entities via restricted Glide queries
B. Custom integration spokes in Integration Hub for one-way data flows from ITSM to GRC
C. Risk Indicator extensions partitioned by domain, correlating with ITSM Vulnerability Items
D. Encrypted field-level access on Control tables synced with ITSM patch management workflows

Answer: B, C, D

Explanation: Custom Integration Hub spokes enforce one-way data flows from ITSM Vulnerability Response (vuln table) to GRC, using air-gapped endpoints to push only anonymized correlations into Risk Indicators, preserving classification levels in defense scenarios. Risk Indicator extensions (sn_risk_indicator) are partitioned by domain in the data model, allowing secure correlation with ITSM Vulnerability Items without exposing full entity details, enabling prioritized patching based on risk

scores. Encrypted field-level access on Control tables (sn_grc_control) integrates with ITSM workflows via scoped APIs, ensuring patch validations occur within isolated domains while updating control effectiveness. Xanadu's partitioning advancements secure these flows, aligning with ServiceNow's high-security architecture patterns.

Question: 1464

How does ServiceNow facilitate the integration of Advanced Risk assessments with third-party ERM tools?

A. By prohibiting external system connections
B. Through open APIs and standardized data formats
C. By manual data export only
D. By using distinct risk vocabularies

Answer: B

Explanation: ServiceNow supports integration through APIs and data standards, enabling seamless data exchange and harmonized risk management across systems.

Question: 1465

Which ServiceNow table serves as the base for storing risk frameworks?

A. grc_framework
B. risk_framework
C. grc_risk_framework
D. grc_risk_model

Answer: C

Explanation: The grc_risk_framework table is the primary table used within ServiceNow GRC to store and manage risk frameworks configurations.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllbus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.