Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

IIA-CRMA MCQs
IIA-CRMA Exam Questions
IIA-CRMA Practice Test
IIA-CRMA TestPrep
IIA-CRMA Study Guide

PASS

killexams.com

IIA

IIA-CRMA 2026

Certification in Risk Management Assurance

100%

BEST

100%

Qustion: 1567

A utility company is facing increased regulatory pressure to reduce carbon emissions. The internal audit team is evaluating the risk assessment process, which uses a qualitative scoring system but lacks integration with environmental trend data. Which of the following improvements should be prioritized to strengthen the process?

A. Adopt a quantitative risk assessment model
B. Implement environmental trend analytics
C. Incorporate regulatory change tracking
D. Increase the frequency of risk reviews
E. Standardize risk reporting formats
F. Train staff on qualitative scoring techniques

Answer: B,C

Explanation: Implementing environmental trend analytics would enhance the process by integrating data on carbon emissions and other environmental factors, addressing the noted gap. Incorporating regulatory change tracking is critical to ensure compliance with new emission regulations. Adopting a quantitative risk assessment model could be useful but is not as directly tied to the scenario's focus. Increasing the frequency of risk reviews is less effective without improved data integration. Standardizing risk reporting formats improves consistency but does not address environmental or regulatory risks. Training staff on qualitative scoring techniques is redundant since the process already uses qualitative scoring.

Question: 1568

A multinational corporation is implementing a new enterprise risk management (ERM) framework to address emerging cyber threats. The internal audit team is tasked with evaluating the risk assessment process used by the IT department. The IT department employs a combination of control self-assessment (CSA) workshops and maturity model evaluations but struggles with inconsistent risk scoring across regions. Which approach should the audit team recommend to enhance the effectiveness of the IT department's risk assessment process?

A. Adopt a standardized risk scoring matrix integrated with CSA workshops
B. Conduct continuous monitoring using automated tools without CSA
C. Develop a qualitative risk assessment model excluding maturity evaluations
D. Implement a third-party risk assessment tool to replace CSA workshops
E. Rely solely on maturity model evaluations for risk prioritization
F. Use ad-hoc risk assessments based on regional IT manager inputs

Answer: A

Explanation: A standardized risk scoring matrix integrated with CSA workshops addresses the

inconsistency in risk scoring across regions by providing a uniform framework for evaluating risks while leveraging the participatory benefits of CSA) Continuous monitoring is valuable but does not directly resolve inconsistent scoring in CSA workshops. Excluding maturity evaluations or replacing CSA with third-party tools limits the collaborative and contextual insights gained from CSA) Relying solely on maturity models lacks the granularity needed for specific risk assessments, and ad-hoc assessments would exacerbate inconsistency.

Question: 1569

An organization's risk culture is described as risk-averse, but recent incidents suggest employees are bypassing controls to meet aggressive performance targets. Which actions should the internal audit team recommend to strengthen the risk culture?

A. Conduct a root cause analysis of control bypass incidents
B. Implement performance incentives tied to risk management adherence
C. Increase the frequency of risk culture assessments
D. Mandate ethics training for all employees
E. Strengthen the tone at the top through leadership messaging
F. Update the risk management framework to include emerging risks

Answer: A,B,C,D,E

Explanation: Conducting a root cause analysis of control bypass incidents identifies underlying issues driving the behavior, enabling targeted improvements. Implementing performance incentives tied to risk management adherence aligns employee goals with risk culture objectives. Increasing the frequency of risk culture assessments helps monitor and address cultural shifts. Mandating ethics training reinforces a risk-aware mindset. Strengthening the tone at the top through leadership messaging sets a positive example, as leadership behavior significantly influences culture. Updating the risk management framework is important but less directly tied to addressing the specific cultural issue of control bypass.

Question: 1570

To provide assurance on a healthcare organization's risk management processes for patient data privacy, which competencies should the internal audit team develop or procure?

A. Strategic risk assessment and corporate governance expertise
B. Financial risk assessment skills and stakeholder communication
C. General IT auditing skills and project management expertise
D. Operational risk framework knowledge and data analytics skills
E. Cybersecurity expertise and knowledge of healthcare regulations

F. Supply chain risk management and internal control knowledge

Answer: E

Explanation: Patient data privacy risks demand specialized competencies. Cybersecurity expertise is critical for assessing technical controls, while knowledge of healthcare regulations ensures compliance with laws like HIPAA.

Question: 1571

The CAE identifies that the internal audit activity's functional reporting to the audit committee is compromised due to the committee's limited risk management expertise. This has led to inadequate oversight of high-risk audit engagements. How should the CAE evaluate and address this independence impairment?
A. Engage external consultants to oversee high-risk engagements
B. Document the issue and adjust engagement scope independently
C. Escalate the concern to the CEO for resolution
D. Assess the audit committee's composition and recommend training
E. Monitor the situation and report to the board only if issues persist
F. Revise the audit charter to limit audit committee responsibilities

Answer: D

Explanation: The audit committee's limited expertise impairs functional reporting, affecting independence per IIA Standard 1111. Assessing the audit committee's composition and recommending training directly addresses the root cause by enhancing oversight capability.

Question: 1572

An energy company is coordinating risk assurance efforts across multiple assurance providers, including internal audit, external audit, and a third-party compliance consultant. You are tasked with ensuring effective coordination. Which of the following actions would best facilitate this coordination?

A. Assigning all assurance activities to the internal audit team
B. Developing a shared assurance framework with defined roles
C. Holding monthly meetings with all assurance providers
D. Outsourcing all assurance activities to a single provider
E. Requiring each provider to submit independent reports
F. Standardizing risk assessment tools across all providers

Answer: B

Explanation: Developing a shared assurance framework with defined roles is the best approach to facilitate coordination, as it clarifies responsibilities, aligns methodologies, and minimizes duplication, aligning with IIA guidance on combined assurance. Assigning all assurance activities to the internal audit team undermines external expertise. Holding monthly meetings with all assurance providers fosters communication but lacks structure. Outsourcing all assurance activities to a single provider reduces diversity of perspectives. Requiring each provider to submit independent reports may lead to silos. Standardizing risk assessment tools across all providers is helpful but insufficient without a broader framework.

Question: 1573

A financial institution's integrated risk management reports are criticized for being too compliance-focused. The internal audit team is tasked with improving these reports. Which of the following deficiencies most likely contributes to this issue?

A. Use of complex technical terminology
B. Inconsistent use of risk metrics across departments
C. Lack of predictive analytics in risk reporting
D. Limited stakeholder engagement in report development
E. Overemphasis on regulatory risk metrics
F. Failure to align risks with strategic business objectives

Answer: F

Explanation: The failure to align risks with strategic business objectives most likely contributes to the compliance-focused nature of the reports, as stakeholders need to understand how risks impact broader goals beyond compliance. Inconsistent metrics, lack of predictive analytics, limited stakeholder engagement, overemphasis on regulatory metrics, and technical terminology are concerns, but alignment with strategic objectives is the primary driver of balanced, strategic reporting.

Question: 1574

An insurance company is coordinating risk assurance efforts and must decide whether to rely on an external auditor's report on financial controls. The report lacks detailed testing procedures. What should you do to assess reliance on this report?

A. Accept the report if the auditor is a recognized industry leader
B. Compare the report's findings with internal audit's findings

C. Validate the report’s conclusions with management
D. Review the auditor’s qualifications and certifications
E. Request the auditor’s detailed testing procedures
F. Verify the auditor’s independence through a third party

Answer: E

Explanation: Request the auditor’s detailed testing procedures is the most appropriate action, as it allows you to evaluate the report’s reliability and alignment with IIA standards. Accepting the report if the auditor is a recognized industry leader overlooks methodological rigor. Comparing the report’s findings with internal audit’s findings is useful but secondary to understanding the procedures. Reviewing the auditor’s qualifications and certifications does not address the report’s content. Validating the report’s conclusions with management risks bias. Verifying the auditor’s independence through a third party is unnecessary without first assessing the procedures.

Question: 1575

An internal audit team at a government agency is evaluating its risk assessment process for procurement fraud. The process uses control self-assessments (CSAs) but lacks quantitative risk measures. Which enhancements should the team recommend?

A. Implement a continuous monitoring system with anomaly detection for procurement transactions
B. Introduce a risk scoring model using decision trees for fraud probability
C. Perform benchmarking against leading public sector procurement processes
D. Use budget vs. actual analysis to evaluate procurement compliance costs
E. Utilize a risk maturity model aligned with COSO ERM
F. Conduct ratio estimation to quantify procurement fraud rates

Answer: A,B,C,E

Explanation: Implement a continuous monitoring system with anomaly detection for procurement transactions provides real-time quantitative risk data.
Introduce a risk scoring model using decision trees for fraud probability quantifies fraud risks.
Perform benchmarking against leading public sector procurement processes identifies best practices.
Utilize a risk maturity model aligned with COSO ERM assesses process maturity.
Use budget vs. actual analysis to evaluate procurement compliance costs focuses on financial metrics, not risk quantification.
Conduct ratio estimation to quantify procurement fraud rates is a sampling technique, not a comprehensive risk measure.

Question: 1576

A healthcare organization is establishing a risk management strategy to address regulatory and operational risks. The board requests your recommendation on integrating risk management with decision-making processes. Which of the following actions would best achieve this integration?

A. Conducting annual risk reviews with the board
B. Outsourcing risk management to a third-party provider
C. Implementing a risk reporting dashboard for executives
D. Embedding risk assessments in all strategic and operational decisions
E. Requiring risk training for all board members
F. Standardizing risk reports across all departments

Answer: D

Explanation: Embedding risk assessments in all strategic and operational decisions ensures risk management is a core component of decision-making, aligning with ISO 31000 principles. Conducting annual risk reviews with the board is too infrequent for integration. Implementing a risk reporting dashboard for executives aids monitoring but not decision-making integration. Outsourcing risk management to a third-party provider reduces internal ownership. Requiring risk training for all board members supports awareness but not integration. Standardizing risk reports across all departments improves consistency but does not embed risk in decision-making.

Question: 1577

A chemical company's operational management systems are audited. You find that safety incident reporting lacks risk controls for underreporting. Which of the following would best integrate risk management into operational systems?

A. Conduct a safety incident risk assessment
B. Implement anonymous reporting channels with KRIs
C. Increase safety training for employees
D. Mandate quarterly safety audits
E. Revise the safety policy to include reporting penalties
F. Use benchmarking to compare incident rates

Answer: B

Explanation: Implementing anonymous reporting channels with KRIs embeds proactive risk controls into safety reporting, enhancing operational integration. A risk assessment is diagnostic but not ongoing. Training improves skills but is less effective than reporting controls. Quarterly audits are reactive. Revising the policy sets rules but doesn't operationalize controls. Benchmarking provides context but

doesn’t address underreporting.

Question: 1578

A pharmaceutical company is assessing risks in its supply chain for raw materials. The risk management team uses a maturity model but lacks real-time supplier monitoring. Which approach should the auditor recommend to enhance risk assessment?

A. Implement continuous monitoring with supplier analytics
B. Conduct control self-assessment (CSA) workshops
C. Rely on external supplier audits
D. Replace maturity models with qualitative reports
E. Use historical supplier data for risk scoring
F. Adopt a static risk register

Answer: A

Explanation: Continuous monitoring with supplier analytics provides real-time insights, enhancing the maturity model. CSA workshops are periodic. External audits are not continuous. Qualitative reports lack analytical rigor. Historical data is backward-looking, and a static risk register is not dynamic.

Question: 1579

A telecommunications company is auditing its network security risk management process. The audit team uses trend analysis to monitor cyber incidents but needs to predict vulnerabilities. Which data analytics techniques should the team adopt?

A. Machine learning for vulnerability prediction
B. Monte Carlo simulation for impact assessment
C. Ratio estimation for security investment
D. Sensitivity analysis for system dependencies
E. Trend analysis of incident frequency
F. Variance analysis of security budgets

Answer: A,B,D

Explanation: Machine learning predicts vulnerabilities based on patterns. Monte Carlo simulation assesses potential impact scenarios. Sensitivity analysis evaluates system dependency risks. Trend analysis tracks incident frequency but is less predictive. Ratio estimation and variance analysis focus on financial metrics, not vulnerability prediction.

Question: 1580

A chemical manufacturer is implementing a risk management framework to address risks from regulatory changes and supply chain disruptions. The internal audit team is assessing whether the framework captures risks from market trends. The team finds that the framework uses a static risk universe and does not incorporate supply chain analytics. What is the most effective recommendation to enhance the framework?

A. Conduct a gap analysis against supply chain standards
B. Develop a dynamic risk universe with supply chain analytics
C. Implement a supply chain monitoring dashboard
D. Increase the frequency of risk assessments
E. Realign the framework with corporate strategy
F. Train staff on supply chain risk analysis

Answer: B

Explanation: Developing a dynamic risk universe with supply chain analytics directly addresses the framework's failure to incorporate supply chain data, ensuring timely risk identification. Conducting a gap analysis against supply chain standards is useful but less immediate. Implementing a supply chain monitoring dashboard focuses on monitoring, not identification. Increasing the frequency of risk assessments is insufficient without analytics. Realigning the framework with corporate strategy is too broad. Training staff on supply chain risk analysis enhances skills but does not improve the framework's design.

Question: 1581

During an audit of a financial institution's compliance with new regulatory requirements, the audit manager identifies gaps in training programs. To ensure audit objectives and quality, which of the following should the manager prioritize?

A. Assign the audit to a single compliance expert
B. Outsource the audit to a regulatory consulting firm
C. Limit the audit to training program deficiencies
D. Conduct a quality assurance review at each audit phase
E. Rely on the compliance team's self-assessment
F. Use automated tools for all compliance testing

Answer: D

Explanation: Conducting a quality assurance review at each audit phase ensures that gaps in training programs are thoroughly evaluated, maintaining audit quality. Assigning the audit to a single expert limits perspectives. Limiting the audit to training deficiencies may miss broader compliance issues. Outsourcing does not develop internal capabilities. Relying on the compliance team's self-assessment lacks independence. Using automated tools alone may overlook complex regulatory requirements.

Question: 1582

A global bank's risk management function is audited. You find that the performance management system does not penalize excessive risk-taking in trading activities. Which of the following recommendations would most effectively integrate risk management into performance management?

A. Conduct a risk culture assessment for the trading team
B. Revise the trading policy to include risk limits
C. Increase risk training for trading staff
D. Mandate quarterly risk reviews by the board
E. Implement clawback provisions for bonuses tied to risk violations
F. Use trend analysis to monitor trading risks

Answer: E

Explanation: Implementing clawback provisions for bonuses tied to risk violations directly aligns performance incentives with risk management, deterring excessive risk-taking. A risk culture assessment diagnoses issues but doesn't change incentives. More training enhances awareness but lacks performance impact. Quarterly board reviews provide oversight but don't address trader behavior. Revising the trading policy sets rules but doesn't incentivize compliance. Trend analysis monitors risks but doesn't integrate with performance systems.

Question: 1583

An organization's new cloud-based collaboration platform lacks robust data privacy controls. Which of the following findings indicates the most critical compliance risk?

A. Absence of a data protection impact assessment (DPIA) for the platform
B. Failure to update the project risk register in the past year
C. Lack of employee training on platform usage
D. No formal change control process for platform updates
E. Outdated vendor contract terms for data security

F. Unclear procedures for user access reviews

Answer: A

Explanation: The absence of a DPIA is the most critical compliance risk, as it is a key requirement under data privacy regulations to assess and mitigate risks to personal data. Failure to update the risk register and lack of training are concerns but less directly tied to compliance. No change control process and unclear access reviews are governance issues. Outdated vendor contracts are a risk but less critical than the absence of a DPIA.

Question: 1584

The CAE discovers that the internal audit activity's independence is impaired because the CEO directs the CAE to exclude certain high-risk areas from the audit plan to avoid scrutiny. How should the CAE address this impairment?

A. Adjust the audit plan and document the CEO's directive internally
B. Disclose the impairment to the audit committee and seek guidance
C. Escalate the issue to the external auditors for resolution
D. Implement alternative assurance procedures for high-risk areas
E. Monitor the situation without immediate action
F. Revise the audit charter to clarify independence requirements

Answer: B,F

Explanation: The CEO's directive compromises independence per IIA Standard 1110. Disclosing the impairment to the audit committee and seeking guidance ensures appropriate oversight and resolution. Revising the audit charter to clarify independence requirements reinforces governance.

Question: 1585

An organization's new CRM system has been flagged for potential cybersecurity vulnerabilities. Which of the following controls should the auditor recommend to strengthen the system's information security policies?

A. Conduct regular penetration testing to identify vulnerabilities
B. Implement encryption for all customer data at rest and in transit
C. Require annual updates to the project risk register
D. Train employees on change management processes
E. Deploy a web application firewall (WAF) to protect against attacks
F. Update the vendor contract to include security clauses

Answer: A,B,E

Explanation: Conducting regular penetration testing identifies vulnerabilities for remediation. Implementing encryption protects customer data confidentiality. Deploying a WAF safeguards against web-based attacks. Updating the risk register is a governance activity, not a security control. Training on change management addresses process risks, not cybersecurity. Updating vendor contracts is contractual, not a direct technical control.

Question: 1586

A government agency is developing a risk management framework to comply with new cybersecurity regulations. The internal audit team is reviewing the framework's ability to assess risks from regulatory changes and emerging threats. The team finds that the framework uses a static risk assessment model that does not incorporate threat intelligence or regulatory updates. What is the most effective recommendation to enhance the framework?

A. Develop a dynamic risk assessment model
B. Conduct a gap analysis against cybersecurity standards
C. Implement a compliance monitoring dashboard
D. Increase the frequency of risk reviews
E. Train staff on regulatory compliance
F. Update the risk appetite statement

Answer: A

Explanation: Developing a dynamic risk assessment model addresses the framework's limitation by incorporating real-time threat intelligence and regulatory updates, ensuring responsiveness to new cybersecurity regulations. Conducting a gap analysis against cybersecurity standards is useful but less immediate than a dynamic model. Implementing a compliance monitoring dashboard focuses on monitoring, not assessment. Increasing the frequency of risk reviews is insufficient without dynamic tools. Training staff on regulatory compliance enhances skills but does not improve the model. Updating the risk appetite statement addresses tolerance, not assessment.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, 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.

Exam Questions Based on Current Exam Objectives

Killexams.com provides 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 questions, candidates will become cover the structure, difficulty level, and topic coverage of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Exam MCQs (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 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 & Desktop)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Exam Simulator. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions. 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 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 relevant material and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.