DUMPSARENA

Certified in Risk and Information Systems Control

Isaca CRISC

Version Demo

Total Demo Questions: 181

Total Premium Questions: 2402

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Governance	396
Topic 2, IT Risk Assessment	631
Topic 3, Risk Response and Reporting	887
Topic 4, Information Technology and Security	480
Topic 5, Mix Questions	8
Total	2402

QUESTION NO: 1

Which key performance efficiency IKPI) BEST measures the effectiveness of an organization ' s disaster recovery program?

A. Number of service level agreement (SLA) violations

B. Percentage of recovery issues identified during the exercise

C. Number of total systems recovered within tie recovery point objective (RPO)

D. Percentage of critical systems recovered within tie recovery time objective (RTO)

ANSWER: D

Explanation:

Percentage of critical systems recovered within tie recovery time objective (RTO) is the best KPI because it directly measures whether the disaster recovery capability is achieving the business-defined restoration target for the systems that matter most. In disaster recovery, the RTO represents the maximum acceptable time to restore a service or system after a disruption. A recovery program is effective when it can consistently restore critical systems within that agreed timeframe, because this demonstrates alignment with business continuity requirements and risk tolerance. Expressing the measure as a percentage is especially useful for management reporting because it shows performance across the critical systems portfolio, supports trend analysis over multiple exercises or incidents, and highlights whether recovery capability is improving or degrading. This KPI also ties technical recovery execution to business impact: critical systems restored within RTO help limit downtime, operational disruption, regulatory exposure, and financial loss. ISACA's glossary recognizes recovery time objective as a key continuity and recovery concept, and NIST disaster recovery guidance similarly emphasizes defining recovery objectives and validating recovery capabilities through testing and exercises. References: ISACA Glossary and NIST SP 800-34 Rev. 1.

QUESTION NO: 2

Which of the following are true for quantitative analysis?

Each correct answer represents a complete solution. (Choose three.)

A. Determines risk factors in terms of high/medium/low.

B. Produces statistically reliable results

C. Allows discovery of which phenomena are likely to be genuine and which are merely chance occurrences

D. Allows data to be classified and counted

ANSWER: B C D

Explanation:

Quantitative analysis is based on measurable, numerical data and uses mathematical or statistical techniques to support conclusions. "Produces statistically reliable results" is correct because quantitative methods are designed to apply repeatable calculations, sampling, probability, distributions, and other statistical techniques to reduce subjectivity and produce results that can be tested or validated. "Allows discovery of which phenomena are likely to be genuine and which are merely chance occurrences" is also correct because statistical analysis helps determine whether observed patterns, correlations, or differences are significant or likely to have occurred randomly. "Allows data to be classified and counted" is correct because quantitative work depends on converting observations into structured data that can be categorized, measured, counted, compared, and analyzed across populations or scenarios. In risk management, this supports numerical estimates such as frequency, impact, exposure, likelihood, and loss magnitude, which are central to quantitative risk analysis. This aligns with recognized risk assessment guidance such as NIST SP 800-30 Revision 1, which describes quantitative assessment as using numerical values and analysis methods, and with ISACA's risk-focused CRISC context described on the ISACA CRISC credential page.

QUESTION NO: 3

A risk owner has accepted a high-impact risk because the control was adversely affecting process efficiency. Before updating the risk register, it is MOST important for the risk practitioner to:

A. ensure suitable insurance coverage is purchased.

B. negotiate with the risk owner on control efficiency.

C. reassess the risk to confirm the impact.

D. obtain approval from senior management.

ANSWER: D

Explanation:

obtain approval from senior management.

is correct because acceptance of a high-impact risk must be supported by an accountable decision at the appropriate level of authority before it is formally recorded as the current risk disposition. In CRISC-aligned risk management practice, the risk practitioner facilitates and documents risk decisions, but acceptance of significant residual risk should be made by management with sufficient authority to understand the business consequences and confirm that the exposure is within the organization's risk appetite and tolerance. Since the reason for accepting the risk is operational efficiency, senior management must weigh the trade-off between business performance and potential impact. Once that approval is obtained, updating the risk register becomes an accurate record of an authorized risk response rather than merely documenting an informal preference. This aligns with broader risk governance principles that require risk decisions to be owned, approved, and monitored by appropriate management stakeholders. NIST guidance similarly emphasizes that senior officials or authorizing officials are responsible for accepting organizational risk after considering mission and business impacts; see NIST SP 800-39 and NIST SP 800-37 Rev. 2.

QUESTION NO: 4

What are the responsibilities of the CRO?

Each correct answer represents a complete solution. (Choose three.)

A. Managing the risk assessment process

B. Implement corrective actions

C. Advising Board of Directors

D. Managing the supporting risk management function

ANSWER: A C D

Explanation:

The correct responsibilities are Managing the risk assessment process, Advising Board of Directors, and Managing the supporting risk management function. In an ISACA-aligned risk governance model, the chief risk officer is the senior executive responsible for coordinating enterprise risk management activities and ensuring that risk practices are consistently applied across the organization. Managing the risk assessment process is a core CRO responsibility because the CRO helps establish the methodology, coordinates assessment activities, and ensures that risk information is reliable enough to support decision-making. Advising Board of Directors is also correct because the CRO provides independent risk insight to executive management and the board, helping them understand the organization's risk profile, significant exposures, and alignment with risk appetite. Managing the supporting risk management function is correct because the CRO typically leads or oversees the risk management function, including policies, processes, reporting, and coordination among risk owners. ISACA's risk guidance emphasizes governance, communication, risk ownership, and management oversight as key components of effective enterprise risk management. For further context, see ISACA's IT risk resources at ISACA IT Risk and COSO's enterprise risk management overview at COSO ERM Guidance.

QUESTION NO: 5

You are the project manager of your enterprise. You have identified new threats, and then evaluated the ability of existing controls to mitigate risk associated with new threats. You noticed that the existing control is not efficient in mitigating these new risks. What are the various steps you could take in this case? Each correct answer represents a complete solution. (Choose three.)

A. Education of staff or business partners

B. Deployment of a threat-specific countermeasure

C. Modify of the technical architecture

D. Apply more controls

ANSWER: A B C

Explanation:

When newly identified threats are not adequately mitigated by existing controls, the appropriate response is to adjust the risk treatment approach so that the enterprise's residual risk remains within tolerance. Education of staff or business partners is correct because many threat scenarios involve human behavior, process awareness, vendor interaction, or operational discipline; targeted awareness and training can directly reduce likelihood or impact. Deployment of a threat-specific countermeasure is correct because a new or changed threat may require a control designed specifically for that threat, rather than relying on a general control that no longer provides sufficient coverage. Modify of the technical architecture is also correct because some risks are best addressed by changing system design, network segmentation, platform configuration, identity architecture, or other structural elements so that exposure is reduced at the source. These responses align with CRISC's focus on identifying, assessing, and responding to IT risk through appropriate controls and risk treatment, as described by ISACA's CRISC certification overview. They also fit COBIT's governance and management approach, where controls, processes, and technology are adjusted to support enterprise objectives and manage risk effectively; see ISACA COBIT resources.

QUESTION NO: 6

Which of the following are true for threats?

Each correct answer represents a complete solution. (Choose three.)

A. They can become more imminent as time goes by, or it can diminish

B. They can result in risks from external sources

C. They are possibility

D. They are real

E. They will arise and stay in place until they are properly dealt.

ANSWER: A B D

Explanation:

The correct statements are "They can become more imminent as time goes by, or it can diminish," "They can result in risks from external sources," and "They are real." In risk management, a threat is a real circumstance, event, actor, or condition with the potential to exploit a weakness and cause harm to an asset, process, or objective. ISACA-aligned risk thinking treats threats as drivers of risk scenarios: a threat source or threat event can create business impact when it acts against an asset in the presence of relevant conditions. This is why "They are real" is correct: a threat is an existing or credible source of potential harm, not merely the absence of a control. "They can result in risks from external sources" is also correct because threats often originate outside the enterprise, such as cybercriminals, competitors, regulators, suppliers, natural events, or market disruptions. "They can become more imminent as time goes by, or it can diminish" is correct because threat likelihood and urgency are dynamic; threat intelligence, environmental changes, actor motivation, and control improvements

can increase or reduce the immediacy of a threat over time. See the ISACA Glossary and the NIST definition of threat for consistent terminology.

QUESTION NO: 7

Which of the following is the PRIMARY risk management responsibility of the second line in the three lines model?

A. Applying risk treatments

B. Implementing internal controls

C. Monitoring risk responses

D. Providing assurance of control effectiveness

ANSWER: C

Explanation:

Monitoring risk responses is correct because the second line in the Three Lines Model is responsible for providing risk-related expertise, oversight, challenge, and monitoring to help ensure that risk management practices are operating as intended and remain aligned with enterprise objectives and risk appetite. In an ISACA CRISC context, management in the first line owns risk and executes day-to-day risk response activities, while the second line supports and oversees risk governance by defining frameworks, setting policies, monitoring risk exposure, and evaluating whether risk responses are appropriate and effective. This makes monitoring risk responses the primary fit for the second line's role: it does not normally own the risk response execution, but it tracks, reviews, and escalates information about whether those responses are achieving the desired risk outcomes. The IIA's updated Three Lines Model describes second-line roles as providing complementary expertise, support, monitoring, and challenge on risk-related matters, which is consistent with CRISC's emphasis on oversight of risk and control activities. See the IIA Three Lines Model and ISACA's CRISC certification overview for related governance, risk, and control context.

QUESTION NO: 8

When reviewing a report on the performance of control processes, it is MOST important to verify whether the:

A. business process objectives have been met.

B. control adheres to regulatory standards.

C. residual risk objectives have been achieved.

D. control process is designed effectively.

ANSWER: C

Explanation:

Residual risk objectives have been achieved is correct because the purpose of a control process, from a risk management perspective, is to reduce risk to a level that aligns with the organization's risk appetite and tolerance. A performance report should therefore be evaluated primarily against whether the implemented controls are actually producing the intended risk outcome. In CRISC terms, control effectiveness is not just about whether a control exists or appears well designed; it is about whether it reduces the likelihood or impact of risk events so that the remaining, or residual, risk is acceptable to management. This aligns with ISACA's risk-focused view of governance and control, where controls are selected, operated and monitored to support defined risk response objectives. ISACA's glossary defines residual risk as the risk remaining after risk responses have been applied, reinforcing why residual risk is the key measure when assessing control performance. See the ISACA Glossary. Similarly, NIST guidance emphasizes ongoing assessment and monitoring to determine whether controls continue to meet intended security and risk objectives; see NIST SP 800-37 Rev. 2.

QUESTION NO: 9

Which of the following statements are true for risk communication? Each correct answer represents a complete solution. (Choose three.)

A. It requires a practical and deliberate scheduling approach to identify stakeholders, actions, and concerns.

B. It helps in allocating the information concerning risk among the decision-makers.

C. It requires investigation and interconnectivity of procedural, legal, social, political, and economic factors.

D. It defines the issue of what a stakeholder does, not just what it says.

ANSWER: A C D

Explanation:

Risk communication is an ongoing, two-way exchange of risk information among relevant stakeholders, so “It requires a practical and deliberate scheduling approach to identify stakeholders, actions, and concerns.” is correct because effective communication must be planned around who needs the information, when they need it, what decisions they must make, and what concerns may influence their understanding of risk. “It requires investigation and interconnectivity of procedural, legal, social, political, and economic factors.” is also correct because risk messages are not purely technical; they must reflect the operating context, obligations, business impact, stakeholder expectations, and external constraints that shape risk perception and response. “It defines the issue of what a stakeholder does, not just what it says.” is correct because credible risk communication includes observable behavior, accountability, escalation, and response actions, not merely statements or reports. This aligns with ISACA’s view of enterprise IT risk as a business issue requiring stakeholder involvement and informed decision-making, and with widely used risk management guidance that emphasizes communication and consultation throughout risk assessment and treatment. See ISACA’s CRISC overview at ISACA CRISC and NIST guidance on risk assessment communication in NIST SP 800-30 Rev. 1.

QUESTION NO: 10

An organization will be impacted by a new data privacy regulation due to the location of its production facilities. What action should the risk practitioner take when evaluating the new regulation?

A. Perform an analysis of the new regulation to ensure current risk is identified.

B. Evaluate if the existing risk responses to the previous regulation are still adequate.

C. Assess the validity and perform update testing on data privacy controls.

D. Develop internal control assessments over data privacy for the new regulation.

ANSWER: A

Explanation:

Perform an analysis of the new regulation to ensure current risk is identified. is correct because a new regulatory requirement represents a potential change to the organization’s risk environment. The risk practitioner’s first responsibility is to understand the regulation’s applicability, scope, obligations, and potential business impact, then translate those findings into identified and assessed risk. This aligns with the CRISC emphasis on identifying, assessing, and evaluating IT and business risk in context before determining whether existing responses or controls are sufficient. Since the trigger is a new data privacy regulation tied to the location of production facilities, the organization must first analyze how the regulation changes compliance exposure, data processing obligations, reporting requirements, and possible penalties. Only after the current risk is clearly identified can management make informed decisions about risk response, control design, control testing, or remediation priorities. ISACA’s CRISC credential overview emphasizes enterprise IT risk identification and management as a core capability, and COBIT also supports evaluating changes in the business and regulatory environment as part of governance and risk management practices. See ISACA CRISC and ISACA COBIT.

QUESTION NO: 11

An organization is considering outsourcing user administration controls tor a critical system. The potential vendor has offered to perform quarterly sett-audits of its controls instead of having annual independent audits. Which of the following should be of GREATEST concern to me risk practitioner?

A. The controls may not be properly tested

B. The vendor will not ensure against control failure

C. The vendor will not achieve best practices

D. Lack of a risk-based approach to access control

ANSWER: A

Explanation:

The controls may not be properly tested is the greatest concern because self-audits performed by the vendor do not provide the same level of objective assurance as an independent audit. For a critical system, user administration controls directly affect access provisioning, modification, revocation and privileged access management; weaknesses in these areas can materially increase the risk of unauthorized access or misuse. Although quarterly self-audits may sound more frequent, the key issue is the lack of independence and the potential for bias, incomplete scope, inconsistent testing methods or insufficient evidence. A risk practitioner should be most concerned that the organization will not receive reliable assurance over the design and operating effectiveness of the outsourced controls. ISACA's third-party risk guidance emphasizes the importance of assurance and oversight over vendor control environments, particularly when critical services are outsourced: ISACA Journal: Third-Party Risk Management Framework. Independent assessment is also a recognized assurance principle in control evaluation, as reflected in NIST's security and privacy control assessment guidance: NIST SP 800-53 Rev. 5.

QUESTION NO: 12

What are the requirements of monitoring risk?

Each correct answer represents a part of the solution. (Choose three.)

A. Information of various stakeholders

B. Preparation of detailed monitoring plan

C. Identifying the risk to be monitored

D. Defining the project's scope

ANSWER: B C D

Explanation:

Effective risk monitoring requires a clear starting point, a structured approach, and agreed boundaries. **Identifying the risk to be monitored** is correct because monitoring must focus on specific risk scenarios, risk indicators, controls, exposures, or response plans; without a defined risk, the organization cannot determine what evidence to collect or what changes should trigger escalation. **Preparation of detailed monitoring plan** is correct because monitoring should specify responsibilities, frequency, data sources, thresholds, reporting methods, and escalation paths so that risk information is collected consistently and supports management decisions. **Defining the project's scope** is also correct because the monitoring activity must clarify which business processes, systems, assets, controls, locations, and stakeholders are included, ensuring that resources are applied to the intended area and results are meaningful. This aligns with ISACA's CRISC focus on risk monitoring and reporting as part of the risk and control lifecycle, as outlined in the CRISC Exam Content Outline. It is also consistent with broader risk management guidance, where ongoing monitoring is planned and scoped to track changes in risk and control effectiveness, such as in NIST SP 800-37 Rev. 2.

QUESTION NO: 13

You are the project manager for BlueWell Inc. Your current project is a high priority and high profile project within your organization. You want to identify the project stakeholders that will have the most power in relation to their interest on your project. This will help you plan for project risks, stakeholder management, and ongoing communication with the key stakeholders in your project. In this process of stakeholder analysis, what type of a grid or model should you create based on these conditions?

A. Stakeholder power/interest grid

B. Stakeholder register

C. Influence/impact grid

D. Salience model

ANSWER: A

Explanation:

Stakeholder power/interest grid is correct because it is specifically designed to classify stakeholders according to two dimensions: the degree of power or authority they can exercise over the project, and the degree of interest they have in the project's outcomes. For a high-priority, high-profile project, this model helps the project manager identify which stakeholders require the most active engagement, communication, and monitoring because they can significantly influence project direction, risk response, approvals, funding, or acceptance. In practical risk and control management, understanding where stakeholders sit on a power-versus-interest view supports better governance, escalation planning, and communication prioritization. Stakeholders with both high power and high interest are typically managed closely because their decisions, concerns, and support can materially affect whether the project succeeds. This aligns with recognized project management practice for stakeholder analysis, where mapping stakeholders by influence, interest, and engagement needs is used to guide communication and involvement strategies. See the Project Management Institute discussion of stakeholder analysis as a key project practice at PMI and a practical stakeholder mapping overview at Atlassian.

QUESTION NO: 14

Which of the following IS processes provide indirect information?

Each correct answer represents a complete solution. (Choose three.)

A. Post-implementation reviews of program changes

B. Security log monitoring

C. Problem management

D. Recovery testing

ANSWER: A B C

Explanation:

Post-implementation reviews of program changes, Security log monitoring, and Problem management are correct because each can provide indirect evidence about the effectiveness of related information systems controls and processes. Post-implementation reviews of program changes help reveal whether change management, testing, approval, migration, and segregation-of-duties controls operated effectively during the system development or maintenance lifecycle. Security log monitoring provides indirect information about access control, authentication, privileged activity, and other security control performance by showing patterns such as failed access attempts, suspicious activity, or control exceptions. Problem management also provides indirect information because recurring problems, root-cause analysis, and incident trends can indicate weaknesses in underlying IS processes such as operations, configuration management, capacity management, change management, or service continuity.

This aligns with ISACA's risk and control perspective, where monitoring, review, and management processes are used to evaluate whether controls are designed and operating effectively across the enterprise's information and technology environment. ISACA's CRISC certification focuses on identifying, assessing, responding to, and monitoring information

technology risk, while COBIT emphasizes governance and management practices that generate evidence for assurance and control monitoring. See ISACA's CRISC overview at ISACA CRISC and COBIT resources at ISACA COBIT.

QUESTION NO: 15

You work as a project manager for SoftTech Inc. You are working with the project stakeholders to begin the qualitative risk analysis process. Which of the following inputs will be needed for the qualitative risk analysis process in your project?

Each correct answer represents a complete solution. (Choose three.)

A. Project scope statement

B. Cost management plan

C. Risk register

D. Organizational process assets

ANSWER: A C D

Explanation:

Project scope statement, Risk register, and Organizational process assets are correct inputs for performing qualitative risk analysis. Qualitative risk analysis is used to prioritize identified risks by assessing their probability of occurrence and potential impact, often considering factors such as urgency, risk categories, stakeholder risk appetite, and available organizational guidance. The project scope statement is important because it helps define project boundaries, assumptions, constraints, and deliverables, all of which affect how risk impact is understood. The risk register is essential because it contains the identified risks that must be assessed and prioritized during the qualitative analysis process. Organizational process assets are also needed because they provide historical information, risk templates, lessons learned, probability and impact definitions, and other organizational standards that support consistent risk evaluation.

This aligns with widely recognized project risk management practices, where qualitative risk analysis depends on existing project documentation, the current list of identified risks, and organizational knowledge to rank risks for further action. For supporting context, see the Project Management Institute's overview of project risk management at PMI and ISACA's risk-related guidance at ISACA.

QUESTION NO: 16

Which of the following is an IT business owner's BEST course of action following an unexpected increase in emergency changes?

A. Evaluating the impact to control objectives

B. Conducting a root cause analysis

C. Validating the adequacy of current processes

D. Reconfiguring the IT infrastructure

ANSWER: B

Explanation:

Conducting a root cause analysis is the best course of action because an unexpected rise in emergency changes is a warning sign that something systemic may be failing in planning, release management, incident response, requirements definition, or the normal change process. Emergency changes often require expedited approval and may bypass parts of the standard control workflow, so the business owner needs to understand the underlying cause before deciding on remediation. A root cause analysis helps determine whether the increase is driven by recurring incidents, inadequate testing, poor capacity planning, weak change categorization, vendor issues, or other process deficiencies. This aligns with COBIT's risk and control principles: management should analyze events and trends that may indicate risk exposure and then address the causes through appropriate governance and management practices. It is also consistent with service management best

practice, where recurring or significant operational events should be analyzed to identify and eliminate underlying causes rather than only treating symptoms. Useful references include ISACA's COBIT resource overview at ISACA COBIT and ITIL-oriented guidance on problem management and root cause analysis at Atlassian ITSM Problem Management.

QUESTION NO: 17

A risk practitioner is assisting with the preparation of a report on the organization's disaster recovery (DR) capabilities. Which information would have the MOST impact on the overall recovery profile?

A. The percentage of systems meeting recovery target times has increased

B. The number of systems requiring a recovery plan has increased

C. The number of systems tested in the last year has increased

D. The percentage of systems with long recovery target times has decreased

ANSWER: A

Explanation:

The percentage of systems meeting recovery target times has increased is the correct answer because disaster recovery capability is best reflected by whether systems can actually be restored within the recovery objectives established by the business. Recovery target times, such as recovery time objectives, represent the maximum tolerable time for restoring a service after disruption. A higher percentage of systems meeting those targets provides direct evidence that the organization's DR capability is improving across the environment and that recovery performance is aligned with business impact and continuity requirements. This kind of metric is outcome-oriented: it measures achieved recovery performance against defined expectations, which is exactly what an overall recovery profile should emphasize. In ISACA-aligned risk and control thinking, meaningful reporting should focus on performance against risk-based objectives and the ability of controls or response capabilities to reduce business impact. NIST's contingency planning guidance similarly emphasizes defining recovery objectives and validating recovery strategies through testing and recovery performance measurement. See NIST SP 800-34 Rev. 1 and ISACA's glossary reference for recovery-related terminology at ISACA Glossary.

QUESTION NO: 18

Which of the following is the PRIMARY reason to conduct risk assessments at periodic intervals?

A. To ensure emerging risk is identified and monitored

B. To establish the maturity level of risk assessment processes

C. To promote a risk-aware culture among staff

D. To ensure risk trend data is collected and reported

ANSWER: A

Explanation:

To ensure emerging risk is identified and monitored is the correct answer because risk is not static. Business objectives, technology environments, threat actors, regulatory expectations, third-party dependencies and control effectiveness all change over time. Periodic risk assessments help an organization reassess its risk profile in light of these changes, identify new or changing risk scenarios, and determine whether existing responses remain appropriate. This aligns with CRISC and ISACA risk management practices, where ongoing identification, analysis and monitoring of IT risk are essential to keeping risk within the enterprise's risk appetite and supporting informed decision-making. The primary value of repeating assessments at planned intervals is not simply administrative reporting; it is maintaining current visibility into risks that may not have existed, or may not have been material, during the previous assessment cycle. ISACA's CRISC credential emphasizes governance, risk identification, risk assessment and risk response as continuing practices, not one-time activities. NIST guidance similarly treats risk assessment as part of an ongoing risk management process that must account for changes in threats, vulnerabilities, impact and likelihood. See ISACA CRISC and NIST SP 800-30 Rev. 1.

QUESTION NO: 19

Which of the following BEST facilitates the identification of appropriate key performance indicators (KPIs) for a risk management program?

A. Reviewing control objectives

B. Aligning with industry best practices

C. Consulting risk owners

D. Evaluating KPIs in accordance with risk appetite

ANSWER: C

Explanation:

Consulting risk owners is correct because meaningful KPIs for a risk management program must reflect how risk-related activities are actually performed, governed and monitored within the business context. Risk owners are accountable for managing assigned risks and for ensuring that risk responses remain effective, so they are best positioned to identify which measures will show whether risk management activities are producing the intended results. Their input helps ensure KPIs are practical, business-relevant, tied to ownership and capable of supporting management decisions rather than being generic metrics selected in isolation. In ISACA's risk governance approach, ownership and accountability are central to effective risk management, and metrics should support monitoring and communication of risk-related performance. This aligns with the broader principle that risk management is integrated with organizational roles and decision-making, as described in guidance such as the ISACA Glossary and NIST's enterprise risk management guidance in NIST SP 800-39. By involving risk owners, the organization is more likely to define KPIs that are actionable, aligned with assigned responsibilities and useful for tracking whether the risk management program is operating effectively.

QUESTION NO: 20

Which of the following requirements is MOST important to include in an outsourcing contract to help ensure sensitive data stored with a service provider is secure?

A. A third-party assessment report of control environment effectiveness must be provided at least annually.

B. Incidents related to data toss must be reported to the organization immediately after they occur.

C. Risk assessment results must be provided to the organization at least annually.

D. A cyber insurance policy must be purchased to cover data loss events.

ANSWER: A

Explanation:

A third-party assessment report of control environment effectiveness must be provided at least annually is the best requirement because it creates an independent, recurring assurance mechanism over the service provider's security controls. When sensitive data is stored by an outsourcing provider, the customer organization remains accountable for managing the risk, but it has limited direct visibility into the provider's internal processes, technical safeguards, and operating effectiveness. Requiring an annual independent assessment, such as a SOC report or comparable third-party review, helps confirm that controls for confidentiality, access management, monitoring, change management, and data protection are designed appropriately and operating effectively over time. This aligns with third-party risk management good practice: contracts should preserve the organization's right to obtain assurance that supplier controls continue to meet agreed security expectations. NIST guidance on cyber supply chain risk management emphasizes the need to define supplier security requirements and monitor supplier performance throughout the relationship; see NIST SP 800-161 Rev. 1. SOC reporting is also widely used to provide independent assurance over service organization controls, as described by the AICPA SOC suite of services.

QUESTION NO: 21

You are the project manager of GHT project. You have planned the risk response process and now you are about to implement various controls. What you should do before relying on any of the controls?

A. Review performance data

B. Discover risk exposure

C. Conduct pilot testing

D. Articulate risk

ANSWER: A C

Explanation:

Before relying on implemented controls, the project manager should validate that the controls actually operate as intended and produce the expected risk-reduction results. Review performance data is correct because control reliance should be based on evidence, such as operating metrics, exception rates, test results, incident trends, or other performance indicators showing that the control is functioning consistently and effectively. Conduct pilot testing is also correct because a pilot allows the organization to test the control in a limited, lower-risk environment before full dependence is placed on it. This helps confirm whether the control design is practical, whether it integrates properly with processes and systems, and whether it creates any unintended operational issues. In CRISC-aligned risk response practice, control implementation is not complete simply because a control has been selected or deployed; it must be monitored, tested, and supported by evidence before management can reasonably rely on it for risk treatment. This aligns with ISACA's emphasis on risk response and control monitoring in the CRISC body of knowledge, and with broader control assessment guidance such as NIST SP 800-53A, which focuses on determining whether controls are implemented correctly, operating as intended, and producing the desired outcome. References: ISACA CRISC Certification and NIST SP 800-53A Rev. 5.

QUESTION NO: 22

Which of the following assets are the examples of intangible assets of an enterprise?

Each correct answer represents a complete solution. (Choose two.)

A. Customer trust

B. Information

C. People

D. Infrastructure

ANSWER: A B

Explanation:

Customer trust and Information are correct because both represent enterprise assets that create value but do not have a physical form. In CRISC and broader ISACA risk management thinking, an asset is anything of value to the enterprise that may need protection, including nonphysical resources whose loss or compromise can affect objectives. Information is a classic intangible asset: it may be stored on physical media, but the value lies in the data, knowledge, records, designs, plans, or business insight it represents. Its confidentiality, integrity, and availability are therefore central to information systems risk and control. Customer trust is also intangible because it reflects stakeholder confidence, brand credibility, and the organization's relationship capital. Although it cannot be touched or directly measured like equipment, damage to customer trust can result in lost revenue, regulatory scrutiny, customer attrition, and strategic harm. ISACA's glossary supports the broad asset concept used in governance and risk contexts, and NIST also recognizes information as an organizational asset requiring protection. See ISACA Glossary and NIST CSRC Glossary: Information Asset.

QUESTION NO: 23

A risk practitioner has been asked to recommend a key performance indicator (KPI) to assess the effectiveness of a manual process to terminate user access. Which of the following would be the BEST KPI to recommend?

A. Percent increase in number of access termination requests

B. Timeframe of notification from business management to IT

C. Timeframe tram user termination to access revocation

D. Ratio of successful login attempts to unsuccessful log-in attempts

ANSWER: C

Explanation:

The best KPI is “Timeframe tram user termination to access revocation” because it directly measures the control objective of the access termination process: removing access promptly once a user no longer has a business need. In a manual process, the main effectiveness concern is not simply whether a request exists, but how long exposure remains after the user’s termination or role change. A shorter and consistently achieved timeframe indicates the process is operating effectively, while delays highlight residual risk from orphaned or unauthorized accounts. This aligns with recognized access control practices that require organizations to manage account lifecycle events and disable or remove accounts when they are no longer needed. For example, NIST SP 800-53 account management guidance includes disabling accounts associated with terminated or transferred users as part of access control expectations, and CIS Controls emphasize active account management as a core security practice. Measuring elapsed time from termination to revocation provides an actionable, outcome-focused KPI that management can trend, benchmark against service-level targets, and use to drive process improvement. References: NIST SP 800-53 AC-2 Account Management and CIS Control 5: Account Management.

QUESTION NO: 24

The PRIMARY reason for a risk practitioner to review business processes is to:

A. Benchmark against peer organizations.

B. Identify appropriate controls within business processes.

C. Assess compliance with global standards.

D. Identify risk owners related to business processes.

ANSWER: D

Explanation:

Identify risk owners related to business processes is correct because effective risk management depends on clear accountability. In ISACA-aligned practice, risks are not owned by the risk practitioner; they are owned by the business leaders or process owners who have authority over the activities, resources, decisions, and outcomes affected by the risk. Reviewing business processes helps the risk practitioner understand how work is performed, where key decisions are made, which stakeholders can accept or treat risk, and who should be accountable for monitoring and responding to risk conditions. This is especially important in CRISC because risk identification and analysis must be tied to business objectives and organizational accountability, not treated as a purely technical exercise. ISACA’s CRISC exam content emphasizes governance, risk ownership, accountability, and alignment of IT risk with enterprise objectives. Similarly, recognized risk management guidance stresses that roles and responsibilities must be assigned so that risk responses can be selected, approved, implemented, and monitored by the appropriate accountable parties. See the ISACA CRISC Exam Content Outline and NIST SP 800-39 for related guidance on risk governance and organizational accountability.

QUESTION NO: 25

A vendor's planned maintenance schedule will cause a critical application to temporarily lose failover capabilities. Of the following, who should approve this proposed schedule?

A. Business continuity manager

B. Chief risk officer (CRO)

C. IT infrastructure manager

D. Business application owner

ANSWER: D

Explanation:

Business application owner is correct because the planned maintenance introduces a temporary increase in availability risk for a critical business application. In ISACA-aligned risk governance, approval of a schedule that knowingly reduces resilience or failover capability should come from the accountable business owner of the affected application or service. That owner is best positioned to determine whether the business impact, timing, customer effect, operational dependency, and residual risk are acceptable. The decision is not merely a technical scheduling matter; it is a business risk acceptance decision because the application may be exposed to outage or degraded recovery capability during the maintenance window. The business application owner can also ensure the timing aligns with business priorities, approve any compensating measures, and confirm that stakeholders understand the temporary exposure. This aligns with ISACA's view that IT risk should be owned and managed in relation to business objectives and value delivery, as described in ISACA risk resources such as IT Risk. It is also consistent with broader continuity and contingency planning practices, where system and business owners participate in planning and acceptance of continuity-related impacts, as reflected in NIST SP 800-34 Rev. 1.

QUESTION NO: 26

Who is PRIMARILY accountable for identifying risk on a daily basis and ensuring adherence to the organization's policies?

A. Line of defense subject matter experts

B. Third line of defense

C. First line of defense

D. Second line of defense

ANSWER: C

Explanation:

First line of defense is correct because day-to-day risk ownership sits with the business and operational management that perform the work. In the three lines model, the first line owns and manages risk as part of normal operations, including identifying risk, applying controls, following organizational policies, and escalating issues when needed. This aligns with CRISC concepts because risk is most effectively identified and managed closest to the process, system, asset, or business activity where the risk arises. Operational managers and staff are directly responsible for executing processes in accordance with established policies and control requirements, so they are primarily accountable for recognizing risk events and ensuring compliance in daily activities. The risk and compliance functions may support, advise, monitor, and challenge, but primary accountability for routine risk identification and policy adherence remains embedded in the first line. This interpretation is consistent with the Institute of Internal Auditors' Three Lines Model, which states that first line roles manage risk and maintain effective controls, and with ISACA guidance on governance and risk practices emphasizing management's responsibility for operating controls and managing enterprise risk. See the IIA Three Lines Model and ISACA Journal discussion of the three lines of defense.

QUESTION NO: 27

When performing a risk assessment of a new service to support a ewe Business process. which of the following should be done FRST10 ensure continuity of operations?

A. a identity conditions that may cause disruptions

B. Review incident response procedures

C. Evaluate the probability of risk events

D. Define metrics for restoring availability

ANSWER: A

Explanation:

The correct choice is “a identity conditions that may cause disruptions” because continuity planning and risk assessment must begin by understanding what could interrupt the new service and the business process it supports. In CRISC-style risk thinking, the first practical step is to identify relevant risk scenarios, threat conditions, vulnerabilities, dependencies, and operational failure points. Only after those disruption conditions are known can the organization meaningfully analyze likelihood, impact, recovery needs, and appropriate controls. For a new service, this includes looking at technology dependencies, third-party services, staffing, facilities, data flows, integration points, and single points of failure that could affect service availability. This aligns with ISACA’s focus on identifying and evaluating IT risk in the context of enterprise objectives, as described in the CRISC exam content. It is also consistent with NIST guidance, which describes risk assessment as starting with the identification of threat sources, threat events, vulnerabilities, and predisposing conditions before determining likelihood and impact; see NIST SP 800-30 Rev. 1.

QUESTION NO: 28

Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

A. Ensuring processes are documented to enable effective control execution

B. Ensuring regular risk messaging is Included in business communications from leadership

C. Ensuring schedules and deadlines for control-related deliverables are strictly monitored

D. Ensuring performance metrics balance business goals with risk appetiie

ANSWER: D

Explanation:

Ensuring performance metrics balance business goals with risk appetiie is the best answer because ethical risk often arises when individuals are held accountable for results without equivalent accountability for how those results are achieved. When control owners are measured only on speed, cost reduction, revenue, or operational throughput, they may feel pressured to bypass controls, underreport issues, or accept risks beyond the organization’s stated tolerance. Balanced performance metrics make control ownership meaningful by aligning incentives with the organization’s risk appetite, reinforcing that risk-aware behavior is part of successful performance rather than an obstacle to it. This is consistent with risk governance principles: risk appetite should guide decisions, priorities, and accountability across the enterprise. ISACA emphasizes the role of risk appetite and tolerance in directing acceptable risk-taking, while ethical expectations require professionals and organizations to act with integrity and due care. See ISACA’s discussion of risk appetite and risk tolerance and the ISACA Code of Professional Ethics.

QUESTION NO: 29

Within the three lines of defense model, the accountability for the system of internal controls resides with:

A. enterprise risk management.

B. the risk practitioner.

C. the chief information officer (CIO).

D. the board of directors.

ANSWER: D

Explanation:

The board of directors is correct because, in the three lines of defense model, the governing body retains ultimate accountability for governance, risk oversight and the effectiveness of the organization's system of internal control. Management and risk functions may design, operate, monitor and report on controls, and internal audit may provide independent assurance, but those activities support the board's oversight role rather than replacing it. The board is expected to ensure that appropriate governance structures are in place, that responsibilities are clearly assigned and that management maintains an effective control environment aligned with organizational objectives and risk appetite. This aligns with the Institute of Internal Auditors' Three Lines Model, which identifies the governing body as accountable to stakeholders for organizational oversight, and with ISACA's governance guidance emphasizing board-level accountability for directing and monitoring enterprise governance. See the IIA Three Lines Model and ISACA COBIT resources for related governance and accountability principles.

QUESTION NO: 30

What should be considered while developing obscure risk scenarios?

Each correct answer represents a part of the solution. (Choose two.)

A. Visibility

B. Controls

C. Assessment methods

D. Recognition

ANSWER: A D

Explanation:

Visibility and Recognition are correct because obscure risk scenarios deal with unlikely, non-historical, or weak-signal events that may not appear in normal loss history or routine risk registers. In ISACA-style risk scenario development, the organization must first have enough Visibility to notice that something unusual or adverse is occurring. This means the enterprise needs sufficient monitoring, environmental awareness, stakeholder input, threat intelligence, operational reporting, and escalation paths to see early indicators of emerging risk. Recognition is equally important because simply observing an event is not enough; the organization must be able to interpret what it sees as a meaningful risk signal. Recognition depends on risk awareness, informed judgment, scenario analysis capability, and an understanding of business context so that unusual observations are identified as potential risk events rather than ignored as noise. Together, Visibility and Recognition help an enterprise imagine and evaluate events that have not yet happened but could still affect objectives. This aligns with ISACA's risk scenario approach, which emphasizes using structured scenarios to identify and analyze possible business impacts. See ISACA's overview of risk scenarios in the Risk IT Framework discussion and ISACA's glossary resources for related risk terminology.

QUESTION NO: 31

Which of the following presents the GREATEST challenge to managing an organization's end-user devices?

A. Incomplete end-user device inventory

B. Unsupported end-user applications

C. Incompatible end-user devices

D. Multiple end-user device models

ANSWER: A

Explanation:

Incomplete end-user device inventory is the correct answer because effective device management depends first on knowing which devices exist, who owns or uses them, where they are located, how they connect, and what their security posture is. Without a complete and accurate inventory, the organization cannot reliably enforce configuration standards, deploy patches, monitor compliance, validate endpoint protection coverage, or assess risk exposure. This creates blind spots: unmanaged laptops, mobile devices, virtual endpoints, or personally owned devices may continue to access organizational data without appropriate controls. From a risk management perspective, asset identification is foundational because risk cannot be measured or treated consistently when the affected assets are unknown or incorrectly recorded. This aligns with widely accepted cybersecurity practices, including the NIST Cybersecurity Framework's emphasis on identifying assets as part of organizational risk management and the CIS Controls' focus on maintaining an accurate enterprise asset inventory. See the NIST Cybersecurity Framework and CIS Control: Inventory and Control of Enterprise Assets for supporting guidance.

QUESTION NO: 32

Which of the following should be the risk practitioner s FIRST course of action when an organization has decided to expand into new product areas?

A. Identify any new business objectives with stakeholders.

B. Present a business case for new controls to stakeholders.

C. Revise the organization's risk and control policy.

D. Review existing risk scenarios with stakeholders.

ANSWER: A

Explanation:

Identify any new business objectives with stakeholders is correct because risk management must begin with a clear understanding of what the organization is trying to achieve. Expansion into new product areas can introduce new revenue goals, customer segments, regulatory obligations, operational dependencies, technology needs and strategic priorities. Before a risk practitioner can assess risk, update scenarios, recommend controls or revise policies, the practitioner needs to understand the business context and objectives that the expansion is intended to support. In ISACA-aligned practice, risk is evaluated in relation to enterprise objectives, risk appetite and stakeholder expectations; therefore, engaging stakeholders first helps ensure that subsequent risk identification and analysis are relevant and business-focused. This approach is consistent with COBIT's emphasis on aligning governance and management of enterprise IT with stakeholder needs and enterprise goals, as described in ISACA's COBIT resources: ISACA COBIT. It also aligns with ISACA's broader risk guidance that effective risk management should be integrated with business decision-making and strategic direction, as discussed in ISACA risk management resources such as Effective Risk Management Through the Risk IT Framework.

QUESTION NO: 33

What are the key control activities to be done to ensure business alignment? Each correct answer represents a part of the solution. (Choose two.)

A. Define the business requirements for the management of data by IT

B. Conduct IT continuity tests on a regular basis or when there are major changes in the IT infrastructure

C. Periodically identify critical data that affect business operations

D. Establish an independent test task force that keeps track of all events

ANSWER: A C

Explanation:

Defining the business requirements for the management of data by IT is correct because business alignment depends on IT managing information in a way that directly supports business objectives, ownership, quality, availability, retention, and compliance needs. In ISACA-aligned governance practice, business requirements should drive IT processes and controls, especially where information is a key enterprise asset. Periodically identifying critical data that affect business operations is also correct because alignment cannot be maintained unless the organization understands which information assets are essential to business processes, risk scenarios, service delivery, and continuity planning. This activity helps ensure that IT priorities, protection levels, recovery objectives, and control investments are focused on data with real business impact. These two control activities connect IT data management to enterprise needs and help ensure that controls are not designed in isolation from operational and risk priorities. ISACA's COBIT materials emphasize aligning governance and management objectives with stakeholder needs and enterprise goals, while CRISC focuses on identifying and managing information systems risk in relation to business objectives. See ISACA's COBIT resources at ISACA COBIT and CRISC credential information at ISACA CRISC.

QUESTION NO: 34

WhichT5f the following is the MOST effective way to promote organization-wide awareness of data security in response to an increase in regulatory penalties for data leakage?

A. Enforce sanctions for noncompliance with security procedures.

B. Conduct organization-w>de phishing simulations.

C. Require training on the data handling policy.

D. Require regular testing of the data breach response plan.

ANSWER: C

Explanation:

Require training on the data handling policy is correct because the issue is organization-wide awareness of data security in the context of increased regulatory exposure from data leakage. A data handling policy defines how employees should classify, access, store, transmit, retain and dispose of sensitive information. Requiring training on that policy directly promotes consistent understanding of employee responsibilities and expected behaviors across the enterprise, which is essential when regulatory penalties make mishandling data a higher business risk. In ISACA-aligned risk and control practice, awareness and training are core mechanisms for embedding risk ownership and control responsibilities into day-to-day operations, rather than limiting knowledge to security or compliance teams. This also aligns with widely accepted security awareness guidance, which emphasizes role-based communication of policies, procedures and responsibilities so personnel can help protect information assets. See ISACA's CRISC overview for the certification's focus on information systems risk and controls at ISACA CRISC, and NIST's guidance on building information security awareness and training programs at NIST SP 800-50.

QUESTION NO: 35

In an organization where each division manages risk independently, which of the following would BEST enable management of risk at the enterprise level?

A. A standardized risk taxonomy

B. A list of control deficiencies

C. An enterprise risk ownership policy

D. An updated risk tolerance metric

ANSWER: A

Explanation:

A standardized risk taxonomy is correct because enterprise risk management depends on a common language for identifying, classifying, comparing and aggregating risk across organizational units. When each division manages risk independently, risks may be described using different terms, categories, impact scales or assumptions, making it difficult for senior management to understand total exposure, identify concentrations of risk or prioritize response activities consistently. A standardized risk taxonomy creates shared definitions and risk categories so divisional risk information can be rolled up into an enterprise view and reported in a meaningful way. This aligns with recognized risk management practices that emphasize consistent terminology, structured risk identification and comparable reporting as prerequisites for effective governance and decision-making. ISACA's risk-related guidance emphasizes that risk must be communicated in business terms and managed consistently across the enterprise; a common taxonomy supports that objective by enabling integrated reporting and oversight. COSO's enterprise risk management guidance similarly focuses on portfolio-level risk understanding, which requires comparable risk information across business units. See ISACA's risk and governance resources at ISACA Glossary and COSO's ERM guidance at COSO ERM Guidance.

QUESTION NO: 36

Within the three lines of defense model, the responsibility for managing risk and controls resides with:

A. the internal auditor.

B. executive management.

C. the risk practitioner.

D. operational management

ANSWER: D

Explanation:

Operational management is correct because, in the three lines of defense model, day-to-day ownership and management of risk sits closest to the business activities that create or encounter the risk. This first-line role is responsible for identifying risks in processes, designing and operating controls, taking corrective action, and ensuring activities remain aligned with organizational objectives and risk appetite. In CRISC terms, this aligns with the principle that risk is owned by the business: those accountable for business processes are also accountable for managing the associated risk and control environment. The updated IIA Three Lines Model describes management's first-line roles as directly responsible for provision of products and services to clients, including managing risk. This means operational management does not merely support risk management; it actively owns and executes it as part of normal operations. For further reference, see The IIA's Three Lines Model and ISACA's overview of the CRISC certification, which emphasizes enterprise IT risk identification, assessment, response and monitoring.

QUESTION NO: 37

What are the requirements for creating risk scenarios? Each correct answer represents a part of the solution. (Choose three.)

A. Determination of cause and effect

B. Determination of the value of business process at risk

C. Potential threats and vulnerabilities that could cause loss

D. Determination of the value of an asset

ANSWER: B C D

Explanation:

Determination of the value of business process at risk, Potential threats and vulnerabilities that could cause loss, and Determination of the value of an asset are correct because a risk scenario must describe what valuable business resource or process is exposed and what adverse conditions could lead to loss. In ISACA risk management practice, scenarios are used

to make risk analysis concrete by linking business impact to relevant assets, processes, threat events, vulnerabilities and loss outcomes. Establishing the value of the asset or business process gives the scenario business context, helping management understand potential impact in terms such as operational disruption, financial loss, regulatory exposure or reputational damage. Identifying the potential threats and vulnerabilities that could cause loss defines how the scenario could occur and supports later likelihood and impact analysis. This aligns with ISACA's risk-based approach in CRISC, where risk identification and analysis are tied to enterprise objectives and business impact; see ISACA CRISC. It is also consistent with widely accepted risk assessment guidance such as NIST SP 800-30 Rev. 1, which emphasizes identifying threat sources/events, vulnerabilities, affected assets and potential adverse impacts when assessing risk.

QUESTION NO: 38

Following an acquisition, the acquiring company ' s risk practitioner has been asked to update the organization ' s IT risk profile What is the MOST important information to review from the acquired company to facilitate this task?

A. Internal and external audit reports

B. Risk disclosures in financial statements

C. Risk assessment and risk register

D. Business objectives and strategies

ANSWER: C

Explanation:

Risk assessment and risk register is correct because it provides the most direct and complete source of information needed to update an IT risk profile after an acquisition. A risk assessment identifies and analyzes relevant IT-related risk scenarios, including likelihood, impact, existing controls, and residual risk. The risk register then consolidates those results into a structured record that can be compared, integrated, and prioritized within the acquiring organization's existing risk profile. For a CRISC practitioner, this is especially important because the updated profile should reflect the combined organization's actual risk exposure, not only high-level business or reporting information. Reviewing the acquired company's risk assessment and risk register enables the practitioner to understand known threats, vulnerabilities, control gaps, risk ownership, treatment plans, and areas requiring escalation or reassessment after integration. This aligns with ISACA's CRISC focus on identifying, assessing, and managing enterprise IT risk in support of business objectives. See ISACA's CRISC certification overview at ISACA CRISC and ISACA's risk-focused resources at ISACA Resources.

QUESTION NO: 39

In which of the following risk management capability maturity levels does the enterprise takes major business decisions considering the probability of loss and the probability of reward? Each correct answer represents a complete solution. (Choose two.)

A. Level 0

B. Level 2

C. Level 5

D. Level 4

ANSWER: C D

Explanation:

Level 5 and Level 4 are correct because they represent the more mature stages of enterprise risk management capability, where risk is no longer treated only as a compliance or control activity. At these levels, risk information is integrated into management processes and major business decisions are made with an understanding of both downside exposure and upside opportunity. In practical ISACA terms, this means the organization evaluates the probability and impact of potential

loss while also considering the probability and value of expected reward, aligning decisions with risk appetite, business objectives, and value delivery.

At Level 4, risk management is typically measured, managed, and consistently embedded into enterprise decision-making. At Level 5, the capability is optimized and continuously improved, with risk-aware decision-making becoming part of enterprise culture and strategic planning. This aligns with ISACA's emphasis that CRISC professionals support risk-informed decisions across governance, assessment, response, and reporting activities. ISACA's broader governance guidance also connects risk management with value creation and enterprise objectives, as reflected in ISACA CRISC and COBIT resources.

QUESTION NO: 40

An organization discovers significant vulnerabilities in a recently purchased commercial off-the-shelf software product which will not be corrected until the next release. Which of the following is the risk manager's BEST course of action?

A. Review the risk of implementing versus postponing with stakeholders.

B. Run vulnerability testing tools to independently verify the vulnerabilities.

C. Review software license to determine the vendor's responsibility regarding vulnerabilities.

D. Require the vendor to correct significant vulnerabilities prior to installation.

ANSWER: A

Explanation:

Review the risk of implementing versus postponing with stakeholders is the best course of action because the risk manager's role is to facilitate an informed, business-aligned risk decision when a known technology risk cannot be immediately eliminated. In this scenario, the vulnerabilities are significant and the vendor has indicated remediation will not occur until a future release, so management must understand the exposure, potential business impact, available compensating controls, and consequences of delaying implementation. The appropriate next step is not simply a technical or contractual action; it is to present the risk in business terms and support stakeholders in deciding whether to accept, mitigate, transfer, or avoid the risk. This aligns with CRISC's emphasis on risk identification, assessment, response, and communication to support enterprise objectives. Risk decisions should be made by accountable stakeholders and risk owners, with the risk manager providing analysis and recommendations. This approach is also consistent with risk management guidance such as NIST's Risk Management Framework, which emphasizes risk-based decision-making and authorization based on organizational risk tolerance. See ISACA CRISC certification overview and NIST SP 800-37 Rev. 2.

QUESTION NO: 41

Which of the following provides the MOST reliable evidence of a control's effectiveness?

A. A risk and control self-assessment

B. Senior management's attestation

C. A system-generated testing report

D. detailed process walk-through

ANSWER: C

Explanation:

A system-generated testing report provides the most reliable evidence of a control's effectiveness because it is based on objective, repeatable data produced by the system that executed or monitored the control. In control assurance work, evidence is stronger when it is direct, independently generated, complete, and less dependent on personal judgment or management representation. A system-generated report can show actual control operation over a defined period, such as exception handling, automated approvals, access rule enforcement, transaction validation, or monitoring results. This makes

it especially useful for assessing whether the control is operating as intended, not merely whether it is documented or understood. ISACA guidance emphasizes that assurance conclusions should be supported by sufficient and appropriate evidence, and automated or system-derived evidence can be highly persuasive when its source, completeness, and integrity are validated. Similarly, audit evidence standards recognize that more reliable evidence is generally obtained from objective sources and direct testing rather than informal inquiry. See ISACA's audit and assurance resources at ISACA Journal and related assurance concepts in ITAF: A Professional Practices Framework for IT Audit/Assurance.

QUESTION NO: 42

What are the functions of the auditor while analyzing risk?

Each correct answer represents a complete solution. (Choose three.)

A. Aids in determining audit objectives

B. Identify threats and vulnerabilities to the information system

C. Provide information for evaluation of controls in audit planning

D. Supporting decision based on risks

ANSWER: A C D

Explanation:

Risk analysis helps an auditor focus audit work where it matters most. "Aids in determining audit objectives" is correct because risk analysis links audit scope and objectives to the areas with the greatest exposure, ensuring the engagement is not just procedural but targeted toward material threats and potential business impact. "Provide information for evaluation of controls in audit planning" is also correct because understanding likelihood, impact, vulnerabilities and existing safeguards gives the auditor the basis for deciding which controls should be assessed, how much testing is needed and where assurance effort should be concentrated. "Supporting decision based on risks" is correct because risk analysis provides structured information that supports prioritization, resource allocation and recommendations aligned with the organization's risk appetite and business priorities. This approach is consistent with ISACA's risk-based view of governance, assurance and control, where audit planning and assurance activities should be driven by risk and business value. See ISACA's overview of IT risk concepts at ISACA IT Risk and the risk assessment guidance in NIST SP 800-30 Rev. 1.

QUESTION NO: 43

Which of the following represents a vulnerability?

A. An identity thief seeking to acquire personal financial data from an organization

B. Media recognition of an organization's market leadership in its industry

C. A standard procedure for applying software patches two weeks after release

D. An employee recently fired for insubordination

ANSWER: C

Explanation:

A standard procedure for applying software patches two weeks after release represents a vulnerability because it creates a predictable weakness in the organization's control environment. In information risk terms, a vulnerability is a weakness in an asset, process, or control that can be exploited by a threat and may lead to business impact. When patches are delayed as a standard practice, systems may remain exposed to publicly known security flaws after fixes are already available. During that window, attackers can use published exploit details, automated scanning, or proof-of-concept code to compromise affected systems. From a CRISC perspective, this is a risk-related weakness because it affects the likelihood that a threat event could successfully occur and should be evaluated against the organization's risk appetite and patch management requirements. This aligns with the commonly used definition of vulnerability as a weakness that can be exploited, such as the

definition in the NIST CSRC Glossary. ISACA's risk and control guidance also emphasizes identifying weaknesses in processes and controls when assessing IT risk; see ISACA's IT risk resources at ISACA IT Risk.

QUESTION NO: 44

Which of the following parameters are considered for the selection of risk indicators?

Each correct answer represents a part of the solution. (Choose three.)

A. Size and complexity of the enterprise

B. Type of market in which the enterprise operates

C. Risk appetite and risk tolerance

D. Strategy focus of the enterprise

ANSWER: A B D

Explanation:

Size and complexity of the enterprise, Type of market in which the enterprise operates, and Strategy focus of the enterprise are correct because risk indicators should be tailored to the business context in which risk is being monitored. In ISACA-aligned risk management practice, key risk indicators are not selected in isolation; they are chosen so they provide meaningful early warning signals for the organization's objectives, operating model, and exposure profile. A large, complex enterprise typically needs broader and more granular indicators because risk events may arise across many processes, technologies, geographies, and control points. The market in which the enterprise operates also shapes the indicators because regulatory pressure, customer expectations, competitive dynamics, and external threat conditions vary significantly by industry. Strategy focus is equally important because indicators should monitor risks that could affect the achievement of strategic objectives, such as growth, resilience, innovation, compliance, or operational efficiency. This aligns with ISACA guidance that risk management and monitoring should support enterprise objectives and decision-making, as reflected in ISACA's CRISC body of knowledge and risk resources at ISACA CRISC. The broader concept of using measures and indicators for security and risk monitoring is also supported by NIST SP 800-55.

QUESTION NO: 45

Which of the following presents the GREATEST security risk to an organization with a large number of Internet of Things (IoT) devices within its network?

A. Inadequate network bandwidth

B. Lack of interoperability between IoT devices

C. Insufficient IoT policies and procedures

D. Increased maintenance costs for IoT devices

ANSWER: C

Explanation:

Insufficient IoT policies and procedures is the correct answer because a large IoT environment creates broad, distributed exposure that must be governed consistently. IoT devices often have constrained security capabilities, varied patching models, default configurations, embedded credentials, and limited logging. Without defined policies and procedures, the organization lacks a reliable basis for setting minimum security requirements, assigning ownership, approving device onboarding, segmenting networks, managing vulnerabilities, enforcing authentication, monitoring device behavior, and responding to incidents. In CRISC terms, this is a governance and risk management concern: controls are only effective when risk ownership, control objectives, risk response expectations, and operating procedures are clearly established and followed. ISACA's CRISC exam content emphasizes IT risk identification, assessment, response, and reporting within an enterprise governance context, which directly supports the need for formal IoT control direction. NIST also highlights IoT

cybersecurity capabilities such as asset identification, configuration, data protection, interface access control, and software update management, all of which depend on organizational policy and procedures to be consistently implemented. See ISACA CRISC Exam Content Outline and NIST Cybersecurity for IoT Program.

QUESTION NO: 46

Establishing an organizational code of conduct is an example of which type of control?

A. Directive

B. Preventive

C. Detective

D. Compensating

ANSWER: A

Explanation:

Directive is correct because an organizational code of conduct is intended to guide and influence behavior by formally communicating expected standards, values, responsibilities and ethical requirements. In ISACA-style control terminology, directive controls are those that tell people what should be done and establish management's expectations before activities occur. A code of conduct does exactly this: it provides direction to employees, contractors and other stakeholders about acceptable conduct, conflicts of interest, compliance obligations, reporting responsibilities and professional behavior. This supports governance and risk management by creating a clear behavioral baseline that helps align individual actions with organizational objectives and risk appetite. In practice, directive controls often include policies, standards, procedures, training, awareness communications and codes of ethics or conduct. ISACA's governance and control guidance emphasizes that policies and communicated expectations are key mechanisms for directing behavior and supporting enterprise objectives; see the ISACA Glossary for related governance and control terminology. Similarly, NIST describes policy and procedure controls as management mechanisms that define expected behavior and responsibilities; see NIST SP 800-53 Rev. 5.

QUESTION NO: 47

Which of the following statements are true for enterprise's risk management capability maturity level 3?

A. Workflow tools are used to accelerate risk issues and track decisions

B. The business knows how IT fits in the enterprise risk universe and the risk portfolio view

C. The enterprise formally requires continuous improvement of risk management skills, based on clearly defined personal and enterprise goals

D. Risk management is viewed as a business issue, and both the drawbacks and benefits of risk are recognized

ANSWER: A B D

Explanation:

At enterprise risk management capability maturity level 3, risk management has moved beyond isolated or informal activity and has become a defined, repeatable discipline aligned across the enterprise. "Workflow tools are used to accelerate risk issues and track decisions" is correct because level 3 includes defined processes and supporting mechanisms for routing, monitoring, and documenting risk-related issues and decisions. "The business knows how IT fits in the enterprise risk universe and the risk portfolio view" is also correct because this maturity level reflects better integration of IT risk into the broader enterprise risk context, allowing technology-related risk to be understood as part of the organization's overall risk profile. "Risk management is viewed as a business issue, and both the drawbacks and benefits of risk are recognized" is correct because mature risk management at this level recognizes risk as part of value creation and business decision-making, not merely as a compliance or technical concern. This aligns with ISACA's emphasis on integrating IT risk with

enterprise governance and business objectives, as reflected in CRISC and IT risk guidance from ISACA CRISC and ISACA's broader IT risk resources.

QUESTION NO: 48

Which of the following parameters would affect the prioritization of the risk responses and development of the risk response plan? Each correct answer represents a complete solution. (Choose three.)

A. Importance of the risk

B. Time required to mitigate risk.

C. Effectiveness of the response

D. Cost of the response to reduce risk within tolerance levels

ANSWER: A C D

Explanation:

The correct parameters are **Importance of the risk**, **Effectiveness of the response**, and **Cost of the response to reduce risk within tolerance levels**. In CRISC risk response planning, prioritization is driven by how significant the risk is to enterprise objectives, whether the proposed response will meaningfully reduce the risk to an acceptable level, and whether the response is economically justified. **Importance of the risk** is central because higher-impact or higher-likelihood risks generally require earlier or stronger treatment, especially when they exceed risk appetite or tolerance. **Effectiveness of the response** is also essential because a response should be selected and prioritized based on its ability to reduce likelihood, impact, or exposure to the desired residual risk level. **Cost of the response to reduce risk within tolerance levels** matters because ISACA-aligned risk management expects risk treatment decisions to be practical, proportionate, and business-justified rather than control implementation for its own sake. These ideas align with the CRISC focus on risk response and reporting described in ISACA's CRISC exam content outline, and with broader risk treatment principles described in NIST risk management guidance. References: ISACA CRISC Exam Content Outline and NIST SP 800-39.

QUESTION NO: 49

Which of the following are the common mistakes while implementing KRIs?

Each correct answer represents a complete solution. (Choose three.)

A. Choosing KRIs that are difficult to measure

B. Choosing KRIs that has high correlation with the risk

C. Choosing KRIs that are incomplete or inaccurate due to unclear specifications

D. Choosing KRIs that are not linked to specific risk

ANSWER: A C D

Explanation:

Choosing KRIs that are difficult to measure, choosing KRIs that are incomplete or inaccurate due to unclear specifications, and choosing KRIs that are not linked to specific risk are common implementation mistakes because they prevent indicators from giving useful early warning about risk exposure. A KRI should be practical, repeatable, clearly defined and tied to a risk scenario, risk appetite, tolerance, or control objective. If a KRI is difficult to measure, it may not be collected consistently or frequently enough to support timely risk decisions. If its definition, calculation method, source data, threshold, owner, or reporting frequency is unclear, the resulting information may be unreliable and may lead to poor escalation or misinterpretation. If it is not linked to a specific risk, it becomes a generic metric rather than a risk indicator, making it hard for management to understand what action is required. ISACA's risk guidance emphasizes that risk indicators should support risk monitoring and decision-making within an enterprise risk management process; see ISACA's overview of IT risk resources at ISACA IT Risk and its discussion of the Risk IT framework at The Risk IT Framework.

QUESTION NO: 50

Which of the following is the GREATEST risk associated with the transition of a sensitive data backup solution from on-premise to a cloud service provider?

A. More complex test restores

B. Inadequate service level agreement (SLA) with the provider

C. More complex incident response procedures

D. Inadequate data encryption

ANSWER: D

Explanation:

Inadequate data encryption is the greatest risk because moving sensitive backup data to a cloud service provider changes the organization's control boundary and increases reliance on technical safeguards to preserve confidentiality. Backups commonly contain large volumes of production data, historical records, credentials, regulated personal information, intellectual property, and other high-impact content. If this data is not strongly encrypted in transit and at rest, or if encryption keys are not properly managed, an exposure at the provider, misconfiguration, interception, or unauthorized administrative access could result in a major data breach. From a risk management perspective, the impact of compromising a full backup set can be greater than compromising a single application dataset because backups often represent aggregated, complete, and long-retained copies of sensitive information. Cloud security guidance consistently emphasizes encryption and key management as critical controls for protecting cloud-hosted data; see the NIST Guidelines on Security and Privacy in Public Cloud Computing and the Cloud Security Alliance Cloud Controls Matrix. Therefore, inadequate data encryption is the most significant risk in this scenario.

QUESTION NO: 51

Which of the following is the BEST method for assessing control effectiveness?

A. Ad hoc reporting

B. Predictive analytics

C. Continuous monitoring

D. Control self-assessment

ANSWER: C

Explanation:

Continuous monitoring is the best method for assessing control effectiveness because it provides ongoing, timely evidence that controls are operating as intended and that exceptions are being identified quickly. In a CRISC context, control effectiveness is not only about whether a control was designed properly, but whether it continues to reduce risk to an acceptable level in actual operation. Continuous monitoring supports this by using recurring measurements, automated alerts, trend analysis, and defined control indicators to detect deterioration or failure before it becomes a significant risk event. This aligns with ISACA's risk and control governance principles in COBIT, where monitoring, evaluating, and assessing performance and conformance are key to ensuring controls remain aligned with enterprise objectives and risk appetite. It is also consistent with broader control assurance guidance such as NIST SP 800-137, which describes information security continuous monitoring as maintaining ongoing awareness of control effectiveness. See ISACA COBIT and NIST SP 800-137.

QUESTION NO: 52

Which of the following are parts of SWOT Analysis?

Each correct answer represents a complete solution. (Choose four.)

A. Weaknesses

B. Tools

C. Threats

D. Opportunities

E. Strengths

ANSWER: A C D E

Explanation:

SWOT analysis is a structured strategic assessment technique used to understand an organization, initiative, project, or risk scenario by examining four core dimensions: Strengths, Weaknesses, Opportunities, and Threats. Strengths and Weaknesses focus on internal conditions, such as capabilities, resources, limitations, skills, process maturity, or control gaps. Opportunities and Threats focus on external conditions, such as market shifts, regulatory changes, technology trends, competitors, suppliers, or emerging risk events. In an ISACA risk and control context, this type of analysis is useful because it helps connect internal control capability with external business and threat conditions, supporting better risk identification, prioritization, and response planning. The correct parts are therefore Weaknesses, Threats, Opportunities, and Strengths, which together form the acronym SWOT. This aligns with widely accepted strategic planning practice and is consistent with how SWOT is commonly used in governance, risk, and business analysis. For reference, see the Investopedia overview of SWOT analysis and the MindTools SWOT analysis guide.

QUESTION NO: 53

Which of the following is MOST important to review when determining whether a potential IT service provider's control environment is effective?

A. Control self-assessment (CSA)

B. Service level agreements (SLAs)

C. Key performance indicators (KPIs)

D. Independent audit report

ANSWER: D

Explanation:

Independent audit report is correct because it provides objective, third-party assurance over the service provider's control environment. When assessing a potential IT service provider, the key concern is whether controls are suitably designed and operating effectively, especially for services that may affect the organization's confidentiality, integrity, availability, compliance, or continuity obligations. An independent audit report, such as a SOC report or equivalent assurance report, is prepared by qualified auditors using recognized criteria and gives the customer organization a stronger basis for relying on the provider's controls than internally generated information alone. It can help identify the scope of systems reviewed, control objectives tested, exceptions noted, management responses, and whether complementary user entity controls are required. This aligns with third-party risk management good practice, where organizations seek independent assurance before placing reliance on outsourced processes or technology services. For further context, ISACA discusses the importance of assurance in third-party risk management in its guidance on vendor oversight: ISACA Journal. The AICPA also describes SOC reports as assurance reports over service organization controls: AICPA SOC Suite of Services.

QUESTION NO: 54

Which of the following BEST indicates the risk appetite and tolerance level (or the risk associated with business interruption caused by IT system failures?

A. Mean time to recover (MTTR)

B. IT system criticality classification

C. Incident management service level agreement (SLA)

D. Recovery time objective (RTO)

ANSWER: D

Explanation:

Recovery time objective (RTO) is the best indicator because it defines the targeted maximum amount of time a business process, service or IT system can be unavailable after a disruption before recovery is required. In practical risk terms, this is a direct expression of how much interruption the organization is prepared to tolerate for a given system or process. A shorter RTO indicates lower tolerance for downtime and usually justifies stronger, more costly resilience and recovery capabilities; a longer RTO indicates the business can accept a greater interruption window. In ISACA-aligned risk management and business continuity practices, RTO is typically established through business impact analysis and reflects business requirements, not just technical performance. This makes it closely tied to risk appetite and risk tolerance for IT-related business interruption. The concept is also consistent with recognized continuity guidance: NIST defines recovery time objective as the overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or processes, as described in the NIST CSRC Glossary and NIST contingency planning guidance at SP 800-34 Rev. 1.

QUESTION NO: 55

Which of the following, who should be PRIMARILY responsible for performing user entitlement reviews?

A. IT security manager

B. IT personnel

C. Data custodian

D. Data owner

ANSWER: D

Explanation:

Data owner is correct because user entitlement reviews are fundamentally a business accountability activity, not merely a technical access administration task. The data owner is accountable for the value, classification, use and protection requirements of the information, and therefore is best positioned to determine whether a user's current access remains appropriate based on job responsibilities, business need and risk tolerance. In ISACA-aligned governance practices, access rights should be periodically validated by the party accountable for the information or process being accessed, because that party understands the business context behind "need to know" and "least privilege." Technical teams may generate reports, facilitate workflow or implement access changes, but the decision about whether an entitlement is justified should come from the accountable owner of the data or business process. This aligns with COBIT's emphasis on clear ownership, accountability and control over information assets, as described in ISACA COBIT resources. It is also consistent with access control guidance such as NIST SP 800-53, which emphasizes periodic review of accounts and privileges to ensure continued authorization; see NIST SP 800-53 Revision 5.

QUESTION NO: 56

You are working in an enterprise. Your enterprise owned various risks. Which among the following is MOST likely to own the risk to an information system that supports a critical business process?

A. System users

B. Senior management

C. IT director

D. Risk management department

ANSWER: B

Explanation:

Senior management is the best answer because accountability for risk tied to critical business processes must remain with the business leadership that has authority over the enterprise's objectives, resources, and risk appetite. In ISACA's risk governance view, IT-related risk is a business risk, not merely a technical issue. When an information system supports a critical business process, the consequences of failure, compromise, or noncompliance directly affect business performance and strategic objectives. Senior management is therefore responsible for ensuring the risk is identified, evaluated, treated, accepted, or escalated in line with the organization's approved risk appetite and tolerance. This ownership includes making or approving key decisions about mitigation funding, residual risk acceptance, and prioritization against other enterprise risks. ISACA's COBIT guidance emphasizes governance and management accountability for aligning information and technology risk with enterprise goals, while ISACA's IT risk resources describe IT risk as part of overall enterprise risk management. See ISACA COBIT and ISACA IT Risk.

QUESTION NO: 57

The BEST key performance indicator (KPI) to measure the effectiveness of a vendor risk management program is the percentage of:

A. vendors providing risk assessments on time.

B. vendor contracts reviewed in the past year.

C. vendor risk mitigation action items completed on time.

D. vendors that have reported control-related incidents.

ANSWER: C

Explanation:

The percentage of vendor risk mitigation action items completed on time is the best KPI because it directly measures whether the vendor risk management program is driving timely risk treatment. An effective program should not only identify and assess third-party risks, but also ensure that agreed remediation activities are completed within target dates and that residual risk is reduced to an acceptable level. Timely completion of mitigation actions demonstrates that risk responses are being executed, tracked, and governed, which aligns closely with CRISC's focus on risk response, control implementation, and monitoring risk treatment outcomes.

This KPI is outcome-oriented: it indicates whether the organization is reducing vendor-related exposure within expected time frames rather than merely completing administrative activities. Strong vendor risk management depends on tracking remediation commitments, escalation of overdue actions, and evidence that control gaps are being addressed. Guidance on third-party and supply chain risk management emphasizes managing identified risks through response and monitoring activities, such as those described in NIST SP 800-161 Rev. 1 and the CISA ICT Supply Chain Risk Management resources.

QUESTION NO: 58

Which of the following are the MOST important risk components that must be communicated among all the stakeholders?

Each correct answer represents a part of the solution. (Choose three.)

A. Various risk response used in the project

B. Expectations from risk management

C. Current risk management capability

D. Status of risk with regard to IT risk

ANSWER: B C D

Explanation:

The correct risk components to communicate broadly among stakeholders are **Expectations from risk management**, **Current risk management capability**, and **Status of risk with regard to IT risk**. In ISACA-aligned risk governance, communication must ensure that stakeholders understand what the enterprise expects from risk management, including the risk strategy, policies, roles, escalation expectations, awareness activities, and the overall tone for risk-aware decision-making. This creates a common basis for consistent risk behavior across the enterprise.

Current risk management capability is also essential because stakeholders need visibility into how effectively the organization identifies, assesses, responds to, and monitors risk. Communicating capability helps leadership understand whether the risk management function is mature enough to support business objectives and whether improvement is needed. **Status of risk with regard to IT risk** is equally important because stakeholders need a current view of risk exposure, key risk indicators, loss events, root causes, and mitigation progress to make informed decisions. These communication themes align with ISACA's focus on enterprise IT risk governance and CRISC's emphasis on identifying, assessing, responding to, and reporting risk. See ISACA's CRISC overview at ISACA CRISC and its IT risk resources at ISACA IT Risk.

QUESTION NO: 59

Which of the following is the BEST metric to demonstrate the effectiveness of an organization's change management process?

A. Average time to complete changes

B. Increase in the number of emergency changes

C. Percent of unauthorized changes

D. Increase in the frequency of changes

ANSWER: C

Explanation:

Percent of unauthorized changes is the best metric because it directly measures whether the change management process is achieving one of its primary control objectives: ensuring that changes to systems, applications, infrastructure, and production environments are properly reviewed, approved, documented, and traceable before implementation. In an effective change management process, unauthorized changes should be rare or nonexistent because they indicate a breakdown in governance, accountability, and control execution. For CRISC and ISACA-style questions, "effectiveness" generally means the extent to which a process achieves its intended risk and control objectives, not simply how fast or how often the process operates. COBIT's change management guidance under practices such as BAI06 emphasizes managing changes in a controlled manner to reduce the likelihood of disruption, unauthorized modification, and risk exposure. Tracking the percentage of unauthorized changes provides a clear risk-based indicator that management can use to assess whether the process is preventing uncontrolled change activity. See ISACA's COBIT resources at ISACA COBIT and ITIL change enablement guidance at AXELOS ITIL 4 Change Enablement.

QUESTION NO: 60

An organization has recently hired a large number of part-time employees. During the annual audit, it was discovered that many user IDs and passwords were documented in procedure manuals for use by the part-time employees. Which of the following BEST describes this situation?

A. Threat

B. Risk

C. Vulnerability

D. Policy violation

ANSWER: C

Explanation:

Vulnerability is correct because documenting user IDs and passwords in procedure manuals creates a weakness in the organization's access control environment. In CRISC terms, a vulnerability is a condition or weakness that can be exploited by a threat source and may contribute to a risk event. Exposed or shared credentials undermine authentication, confidentiality, and accountability because anyone with access to the manuals could use those credentials without being uniquely identified. The audit finding describes the existence of this weakness itself, not the full business impact or likelihood calculation. ISACA's glossary frames vulnerability as a weakness that may be exploited, while NIST similarly defines it as a weakness in a system, procedure, internal control, or implementation that could be exercised by a threat source. The discovered practice is therefore best categorized as a vulnerability in identity and access management controls. References: ISACA Glossary and NIST CSRC Glossary: Vulnerability.

QUESTION NO: 61

According to the Section-302 of the Sarbanes-Oxley Act of 2002, what does certification of reports implies? Each correct answer represents a complete solution. (Choose three.)

A. The signing officer has evaluated the effectiveness of the issuer's internal controls as of a date at the time to report.

B. The financial statement does not contain any materially untrue or misleading information.

C. The signing officer has reviewed the report.

D. The signing officer has presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date.

ANSWER: B C D

Explanation:

Under Section 302 of the Sarbanes-Oxley Act, the principal executive and financial officers must personally certify key aspects of each periodic report. "The signing officer has reviewed the report" is correct because the statute explicitly requires the certifying officer to state that they have reviewed the report. "The financial statement does not contain any materially untrue or misleading information" is also correct because the certification must state that, based on the officer's knowledge, the report does not include any untrue statement of a material fact or omit a material fact needed to make the statements not misleading. "The signing officer has presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date" is correct because Section 302 requires management to evaluate disclosure controls and procedures and present conclusions about their effectiveness in the report. These certifications are central to SOX's goal of increasing executive accountability over financial reporting, disclosure accuracy, and internal control effectiveness. See the statutory text at 15 U.S.C. § 7241 and the SEC's implementing rule discussion at SEC Final Rule 33-8124.

QUESTION NO: 62

You are the project manager of GHT project. You and your team have developed risk responses for those risks with the highest threat to or best opportunity for the project objectives. What are the immediate steps you should follow, after planning for risk response process? Each correct answer represents a complete solution. (Choose three.)

A. Updating Project management plan and Project document

B. Applying controls

C. Updating Risk register

D. Prepare Risk-related contracts

ANSWER: A C D

Explanation:

Updating Risk register is correct because the planned responses for significant threats and opportunities must be formally captured so they can be assigned, tracked, monitored, and used in later risk control activities. Updating Project management plan and Project document is also correct because agreed risk responses often affect baselines, schedules, budgets, resource plans, assumptions, and related planning artifacts; these updates keep the overall project plan aligned with the selected response strategies. Prepare Risk-related contracts is correct because some responses require third-party involvement, such as transferring risk through insurance, outsourcing specialized work, or sharing an opportunity with another organization. In those cases, procurement or contract-related decisions should be initiated as part of the immediate outputs of planning risk responses. These actions align with standard project risk management practice, where the plan risk responses activity produces updates to the risk register, project management plan, project documents, and procurement-related decisions or contract actions. For broader context on project risk management practices, see the PMI PMBOK Guide and Standards and ISACA's CRISC certification domain focus on IT risk identification, assessment, response, and reporting at ISACA CRISC.

QUESTION NO: 63

You are the project manager of GHT project. Your hardware vendor left you a voicemail saying that the delivery of the equipment you have ordered would not arrive on time. You identified a risk response strategy for this risk and have arranged for a local company to lease you the needed equipment until yours arrives. This is an example of which risk response strategy?

A. Avoid

B. Transfer

C. Acceptance

D. Mitigate

ANSWER: D

Explanation:

Mitigate is correct because the project manager is taking action to reduce the business impact of the delayed equipment delivery. The risk event has not been eliminated, and the original vendor delivery problem may still occur, but arranging leased equipment provides an alternate operational capability so the project can continue with less disruption. In ISACA-aligned risk management, mitigation generally means implementing measures that reduce the likelihood and/or impact of a risk to a level that is acceptable to the organization. This is consistent with CRISC's focus on risk response and reporting, where the selected response should be appropriate to the risk scenario and aligned with business objectives; see ISACA's CRISC overview at ISACA CRISC. A useful general reference for the terminology is the ISACA Glossary, which supports consistent use of risk and control concepts. Leasing substitute equipment is a practical compensating measure: it preserves the project schedule and reduces the consequence of late delivery. Because the action directly lessens the negative effect of the vendor delay on the project, it is best categorized as mitigation.

QUESTION NO: 64

What are the three PRIMARY steps to be taken to initialize the project?

Each correct answer represents a complete solution. (Choose three.)

A. Conduct a feasibility study

B. Define requirements

C. Acquire software

D. Plan risk management

ANSWER: A B C

Explanation:

The correct selections are Conduct a feasibility study, Define requirements, and Acquire software. In an information systems project, initialization begins by confirming that the proposed work is justified, achievable, and aligned with business needs. Conduct a feasibility study is primary because it validates the business case, expected benefits, cost considerations, constraints, alternatives, and whether the project should proceed. Define requirements is also primary because the organization must establish what the solution is expected to accomplish before committing to design, procurement, or development decisions. Requirements provide the basis for scope, acceptance criteria, stakeholder expectations, and later control activities. Acquire software is included because, once feasibility and requirements are established, the organization may determine whether to build, buy, or modify a solution; acquisition planning or procurement becomes a key initialization activity when a packaged or externally supplied solution is selected. This sequence is consistent with IS governance practices that emphasize business alignment, requirements definition, and controlled solution acquisition, as reflected in ISACA COBIT resources. It is also consistent with systems development guidance such as NIST SP 800-64 Rev. 2, which describes early life-cycle activities around initiation, requirements, and acquisition planning.

QUESTION NO: 65

Which of the following are the principles of access controls?

Each correct answer represents a complete solution. (Choose three.)

A. Confidentiality

B. Availability

C. Reliability

D. Integrity

ANSWER: A B D

Explanation:

Confidentiality, Availability, and Integrity are correct because access control is fundamentally designed to protect the core security objectives commonly known as the CIA triad. Confidentiality is supported by access controls that restrict information access to authorized users, processes, or systems, helping prevent unauthorized disclosure of sensitive data. Availability is supported when access control mechanisms ensure legitimate users can obtain timely and reliable access to required systems and information, while also preventing misuse or disruption by unauthorized parties. Integrity is supported by limiting who can create, modify, delete, or approve data and transactions, thereby helping ensure information remains accurate, complete, and protected from unauthorized alteration.

In IS risk and control practice, these three principles are central when designing, assessing, and monitoring logical and physical access controls. They provide the basis for determining whether identities, privileges, authentication, authorization, and monitoring processes are adequately protecting business information assets. NIST's glossary definitions for confidentiality and availability reflect these same security objectives, and integrity is likewise treated as a core information security property.

QUESTION NO: 66

Which of the following role carriers will decide the Key Risk Indicator of the enterprise? Each correct answer represents a part of the solution. Choose two.

A. Business leaders

B. Senior management

C. Human resource

D. Chief financial officer

ANSWER: A B

Explanation:

Business leaders and Senior management are correct because key risk indicators must be tied to the enterprise's objectives, risk appetite, and decision-making needs. In CRISC-aligned risk practice, KRIs are not selected merely because data is available; they are chosen because they provide meaningful early warning that risk exposure may be increasing or that important business objectives may be threatened. Business leaders understand the operational context, critical processes, performance expectations, and risk scenarios that matter most in their areas. Senior management provides the enterprise-level perspective needed to align KRIs with strategic priorities, governance expectations, and accepted risk thresholds. Together, these roles help determine which indicators should be elevated from ordinary metrics, logs, reports, or alerts into KRIs that are monitored and reported regularly. This aligns with ISACA's focus on risk governance, risk monitoring, and business alignment in the CRISC body of knowledge. For additional context, see ISACA's CRISC credential information at ISACA CRISC and ISACA's discussion of key risk indicators at Key Risk Indicators: The Canary in the Coal Mine.

QUESTION NO: 67

An organization is planning to engage a cloud-based service provider for some of its data-intensive business processes. Which of the following is MOST important to help define the IT risk associated with this outsourcing activity?

A. Service level agreement

B. Right to audit the provider

C. Customer service reviews

D. Scope of services provided

ANSWER: D

Explanation:

Scope of services provided is correct because defining IT risk for an outsourcing or cloud engagement starts with understanding exactly what business processes, data, systems, responsibilities, locations, integrations and service boundaries are included. In CRISC terms, effective risk identification and analysis require context: what assets and processes are exposed, how critical they are, who performs which activities, and where control responsibility shifts between the organization and the provider. For data-intensive processes, the scope clarifies the volume and sensitivity of data processed, storage and transmission points, regulatory implications, dependencies, and operational impact if the provider fails. Without this scope, the organization cannot meaningfully identify threats, assess likelihood and impact, determine inherent risk, or select appropriate controls. This aligns with risk assessment guidance that emphasizes understanding system characteristics and organizational context before analyzing risk, as described in NIST SP 800-30 Rev. 1. Cloud-specific guidance also highlights that risks vary significantly depending on the cloud service model, deployment model and allocation of responsibilities, as outlined in NIST SP 800-146.

QUESTION NO: 68

What are the requirements of effectively communicating risk analysis results to the relevant stakeholders? Each correct answer represents a part of the solution. (Choose three.)

A. The results should be reported in terms and formats that are useful to support business decisions

B. Communicate only the negative risk impacts of events in order to drive response decisions

C. Communicate the risk-return context clearly

D. Provide decision makers with an understanding of worst-case and most probable scenarios

ANSWER: A C D

Explanation:

Effective communication of risk analysis results must help stakeholders make informed, risk-aware business decisions. “The results should be reported in terms and formats that are useful to support business decisions” is correct because risk information must be understandable, decision-oriented and aligned with the audience’s responsibilities, not merely technical or analytical. “Communicate the risk-return context clearly” is also correct because management needs to understand likelihood, impact, uncertainty, potential benefit and exposure in a balanced way before selecting an appropriate response. “Provide decision makers with an understanding of worst-case and most probable scenarios” is correct because scenario-based communication gives stakeholders practical insight into the range of possible outcomes, including severe exposure and the most likely business impact. These practices align with the CRISC emphasis on identifying, assessing and communicating IT risk in a way that supports enterprise objectives and governance decisions. They are also consistent with broadly accepted risk assessment guidance, which stresses that risk outputs should be documented and communicated in forms useful to decision makers. See ISACA’s CRISC credential overview at ISACA CRISC and NIST’s risk assessment guidance at NIST SP 800-30 Rev. 1.

QUESTION NO: 69

Which of the following should be the MOST important consideration for senior management when developing a risk response strategy?

A. Cost of controls

B. Risk tolerance

C. Risk appetite

D. Probability definition

ANSWER: C

Explanation:

Risk appetite is the correct choice because it represents the amount and type of risk the enterprise is willing to accept in pursuit of its objectives. A risk response strategy should be designed to bring risk decisions into alignment with that enterprise-level direction. Senior management is responsible for ensuring that risk responses support business objectives and do not result in accepting more risk than the organization has agreed is appropriate. In CRISC terms, risk response is not just a technical control decision; it is a business decision that must reflect the organization’s governance expectations, value delivery goals, and acceptable exposure. Risk appetite provides the strategic boundary for choosing whether to accept, mitigate, transfer, or avoid a risk. ISACA’s risk governance guidance emphasizes that risk-related decisions should be aligned with enterprise objectives and appetite, and NIST also describes risk appetite as a key input for organizational risk decisions. See ISACA Glossary and NIST SP 800-39.

QUESTION NO: 70

Which of the following IT key risk indicators (KRIs) provides management with the BEST feedback on IT capacity?

A. Trends in IT resource usage.

B. Increased resource availability.

C. Trends in IT maintenance costs.

D. Increased number of incidents.

ANSWER: A

Explanation:

Trends in IT resource usage is correct because capacity-related risk is best understood by monitoring how infrastructure, applications, networks, storage, processing power and other IT resources are being consumed over time. A useful KRI should provide early warning and management insight, not just report after a capacity problem has already affected service delivery. Resource usage trends allow management to see whether demand is approaching thresholds, whether growth is accelerating, and whether current capacity plans remain aligned with business requirements. This supports proactive decisions such as scaling infrastructure, tuning workloads, revising service levels or prioritizing investment before performance or availability is degraded.

In CRISC and COBIT-aligned risk management, KRIs are intended to signal changing risk exposure and support timely risk response. Capacity risk is inherently trend-based because a single utilization snapshot may not show whether the environment is stable, under stress or moving toward constraint. ISACA's COBIT guidance emphasizes monitoring performance, capacity and resource optimization as part of governance and management of enterprise IT; see ISACA COBIT resources. ISACA also describes KRIs as measures that help identify potential risk events and changing exposure; see ISACA Journal on key risk indicators.

QUESTION NO: 71

Which of the following aspects are included in the Internal Environment Framework of COSO ERM? Each correct answer represents a complete solution. (Choose three.)

A. Enterprise's integrity and ethical values

B. Enterprise's working environment

C. Enterprise's human resource standards

D. Enterprise's risk appetite

ANSWER: A C D

Explanation:

The correct aspects are Enterprise's integrity and ethical values, Enterprise's human resource standards, and Enterprise's risk appetite. In the COSO ERM model, the internal environment is the foundation for how risk is viewed, governed, and acted on throughout the organization. Integrity and ethical values are central because they shape the organization's risk culture and influence whether personnel make decisions consistent with governance expectations. Human resource standards are also part of the internal environment because hiring, training, performance management, and accountability practices help ensure people have the competence and behavioral expectations needed to support risk management. Risk appetite is included because COSO ERM expects management and the board to establish the amount of risk the entity is willing to accept while pursuing objectives; that appetite then guides strategy, control design, and risk response. Together, these elements set the tone for enterprise risk management before specific events are identified or controls are selected. For reference, COSO describes ERM as an integrated approach to managing risk in support of strategy and performance in its ERM guidance: COSO ERM Guidance. ISACA's CRISC certification also emphasizes governance, risk appetite, and organizational risk practices as core risk management concepts: ISACA CRISC.

QUESTION NO: 72

Who is at the BEST authority to develop the priorities and identify what risks and impacts would occur if there were loss of the organization's private information?

A. External regulatory agencies

B. Internal auditor

C. Business process owners

D. Security management

ANSWER: C

Explanation:

Business process owners is correct because the people who own and manage the business processes are best positioned to determine the value, sensitivity, and operational importance of the information used by those processes. In risk management, impact analysis and prioritization must be driven by business context: what services would be disrupted, what legal or customer obligations would be affected, what financial or reputational harm could result, and how quickly the process must be restored. Business process owners understand these dependencies and can define the business consequences of losing private information more accurately than technical or oversight functions. Security and risk teams can facilitate the assessment, provide methodology, and recommend controls, but the authority for prioritizing business impact belongs with the accountable business owners. This aligns with the ISACA view that governance and risk decisions should be tied to business objectives and ownership, and with business impact analysis practices described by NIST, where organizational mission and business process impacts drive prioritization. See the ISACA Glossary and NIST SP 800-34 Rev. 1 for related guidance.

QUESTION NO: 73

The PRIMARY purpose of using a framework for risk analysis is to:

A. improve accountability

B. improve consistency

C. help define risk tolerance

D. help develop risk scenarios.

ANSWER: B

Explanation:

Using a framework for risk analysis primarily serves to improve consistency. A framework gives the organization a common structure, terminology, criteria and repeatable method for identifying, assessing, comparing and reporting risk. This is especially important in enterprise IT risk management because different business units, systems and processes may otherwise assess likelihood, impact and control effectiveness in different ways, making results difficult to compare or prioritize. When risk analysis is performed consistently, management can aggregate risk information, make informed decisions, allocate resources appropriately and track changes over time. ISACA's risk guidance emphasizes structured approaches to linking IT risk with business objectives and supporting reliable risk-informed decision-making; see the ISACA Risk IT Framework. Similarly, NIST describes risk assessment as a structured process that supports comparable and repeatable risk determinations; see NIST SP 800-30 Revision 1. Therefore, "improve consistency" is the best answer because the central value of a risk analysis framework is enabling repeatable, comparable and defensible analysis across the organization.

QUESTION NO: 74

Which of the following BEST enables a risk practitioner to understand management's approach to organizational risk?

A. Organizational structure and job descriptions

B. Risk appetite and risk tolerance

C. Industry best practices for risk management

D. Prior year's risk assessment results

ANSWER: B

Explanation:

Risk appetite and risk tolerance is the best answer because these concepts directly express how management wants the organization to take, avoid, accept, or respond to risk in pursuit of objectives. Risk appetite communicates the broad amount

and type of risk the enterprise is willing to accept, while risk tolerance translates that appetite into more specific boundaries, thresholds, or acceptable variation from expected outcomes. For a risk practitioner, understanding these statements and limits is essential because they provide the context for evaluating whether identified risks are acceptable, require treatment, or should be escalated. They also guide prioritization of risk responses and help ensure that risk decisions are aligned with business strategy and executive expectations. ISACA guidance consistently treats risk appetite and tolerance as key governance inputs for risk management, because they connect risk assessment and control decisions to the organization's objectives and leadership direction. For additional context, see ISACA's discussion of risk appetite and risk tolerance and ISACA's glossary definitions for core risk terminology.

QUESTION NO: 75

Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

A. Implement segregation of duties.

B. Enforce an internal data access policy.

C. Enforce the use of digital signatures.

D. Apply single sign-on for access control.

ANSWER: B

Explanation:

Enforce an internal data access policy is correct because preventing unauthorized retrieval of confidential information depends primarily on ensuring that access to application data is explicitly governed, authorized, and restricted based on business need. A well-enforced data access policy defines who may access specific types of information, under what conditions, and through which approved mechanisms. In a business application, this typically translates into role-based or attribute-based authorization rules, least-privilege permissions, periodic access reviews, and logging or monitoring to detect inappropriate attempts to retrieve sensitive records. From a CRISC perspective, this is the most appropriate risk response because it directly addresses the confidentiality risk at the point where the information is stored and accessed. ISACA emphasizes the importance of governance and control practices that align access with business requirements and risk appetite, while NIST access control guidance similarly describes enforcing approved authorizations for logical access to information and system resources. See the ISACA Glossary and NIST SP 800-53 Rev. 5 for related access control concepts.

QUESTION NO: 76

Which of the following is the GREATEST risk to an organization when using a public AI system to process credit card transactions?

A. Potential exposure of sensitive information

B. Use of financial data to train the AI model

Use of financial data to train the AI modelis a specific form of data misuse, but it falls within the broader and more critical risk of sensitive information exposure.

C. Noncompliance with security standards

Noncompliance with security standardsis also significant, but it is often a consequence of exposing or improperly handling sensitive payment data.

D. AI hallucinations and bias

AI hallucinations and biasare important AI risks, but they are not the primary concern in payment card processing.
Exact Extracts supporting the answer:
"The MOST important consideration when transmitting personal information across networks is ensuring the privacy of the personal information."

“The data security control that BEST protects the confidentiality of data stored on backup media in transit to a third-party storage facility is encryption.”
“The MOST significant risk associated with handling credit card data through a web application is failure to store credit card data in a secure area segregated from the demilitarized zone.”
“To determine the level of protection required for securing personally identifiable information a risk practitioner should PRIMARILY consider the sensitivity property of the information.”
These extracts support that the primary concern with payment-card-related processing is protecting the confidentiality of sensitive data. Therefore, the greatest risk is thepotential exposure of sensitive information.
==========

ANSWER: A

Explanation:

Potential exposure of sensitive information is the correct answer because credit card transactions involve highly sensitive cardholder data, and submitting that data to a public AI system can create an immediate confidentiality and data-handling risk. Public AI services may process, retain, log, transmit, or otherwise expose submitted prompts and transaction details outside the organization’s controlled environment. From a CRISC risk perspective, the greatest risk is the one with the highest potential business impact: unauthorized disclosure of payment card data can lead to fraud, customer harm, regulatory and contractual consequences, breach notification obligations, financial penalties, and reputational damage. Payment card environments are expected to apply strong controls to protect account data, including limiting storage, transmission, and access based on business need. The PCI Security Standards Council emphasizes protection of cardholder data through the PCI DSS requirements, while the NIST AI Risk Management Framework highlights the need to manage AI-related risks such as privacy, security, and data governance. Therefore, when a public AI system is used in payment processing, the primary and greatest concern is the potential exposure of sensitive information.

QUESTION NO: 77

An organization has recently updated its disaster recovery plan (DRP). Which of the following would be the GREATEST risk if the new plan is not tested?

A. External resources may need to be involved.

B. Data privacy regulations may be violated.

C. Recovery costs may increase significantly.

D. Service interruptions may be longer than anticipated.

ANSWER: D

Explanation:

Service interruptions may be longer than anticipated is the correct answer because the main purpose of disaster recovery planning is to ensure the organization can restore critical systems and services within defined recovery objectives, such as the recovery time objective and recovery point objective. When a disaster recovery plan has been updated but not tested, management has no reliable assurance that procedures, dependencies, roles, communication paths, backup restoration steps, third-party arrangements, and technical recovery sequences will work as expected during an actual disruption. Testing validates whether the plan is executable under realistic conditions and reveals gaps before a real incident occurs. In ISACA-aligned risk thinking, the greatest concern is the business impact created when recovery capabilities fail to meet expectations; prolonged outage time can directly affect operations, customers, revenue, compliance commitments, and stakeholder confidence. Guidance such as NIST SP 800-34 Rev. 1 emphasizes exercising and maintaining contingency plans to ensure recovery strategies remain effective. Similarly, Ready.gov business continuity testing guidance highlights testing and exercises as a way to validate plans and improve response capability.

QUESTION NO: 78

Which of the following should be done FIRST when developing an initial set of risk scenarios for an organization?

A. Consider relevant business activities.

B. Use a bottom-up approach.

C. Use a top-down approach.

D. Refer to industry standard scenarios.

ANSWER: A

Explanation:

Consider relevant business activities is correct because effective risk scenarios must begin with the organization's business context. In ISACA-aligned risk practice, scenarios are not created as generic technical events first; they are framed around what the enterprise does, what objectives it is trying to achieve, which processes and services are most important, and where uncertainty could affect value delivery. Starting with relevant business activities ensures the initial scenarios are meaningful to stakeholders, tied to enterprise objectives, and useful for later risk analysis, assessment, and response. This also helps define the scope of the scenario, including affected processes, information assets, people, technology, third parties, and potential business impacts. The CRISC body of knowledge emphasizes identifying and evaluating IT risk in alignment with enterprise goals and risk appetite, which requires understanding the business activities that create or depend on information systems. This approach is also consistent with broader risk assessment guidance, such as NIST SP 800-30, which frames risk identification around organizational operations, assets, individuals, and mission/business processes. References: ISACA CRISC Certification and NIST SP 800-30 Rev. 1.

QUESTION NO: 79

Which of the following is the BEST way to validate the results of a vulnerability assessment?

A. Perform a penetration test

B. Perform a root cause analysis

C. Conduct a threat analysis

D. Review security logs

ANSWER: A

Explanation:

Perform a penetration test is the best way to validate the results of a vulnerability assessment because it moves beyond identifying potential weaknesses and tests whether those weaknesses can actually be exploited in a realistic manner. A vulnerability assessment typically produces findings based on scanning, configuration review, or known weakness detection. Penetration testing provides validation by attempting controlled exploitation, confirming the practical impact, exploitability, and risk significance of the reported vulnerabilities. This helps risk and security teams distinguish theoretical findings from issues that present demonstrable exposure to the organization.

This aligns with common security assessment guidance: NIST describes penetration testing as security testing in which assessors attempt to circumvent security features based on their understanding of system design and implementation, while technical assessment guidance distinguishes it from broader vulnerability identification activities. See NIST CSRC Glossary: Penetration Testing and NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. In a CRISC context, this supports better risk evaluation because confirmed exploitability improves the quality of risk analysis and treatment decisions.

QUESTION NO: 80

You are the project manager of GHT project. A risk event has occurred in your project and you have identified it. Which of the following tasks you would do in reaction to risk event occurrence? Each correct answer represents a part of the solution. (Choose three.)

A. Monitor risk

B. Maintain and initiate incident response plans

C. Update risk register

D. Communicate lessons learned from risk events

ANSWER: A B D

Explanation:

When a risk event actually occurs, the appropriate response is to move from planning and monitoring into active risk and incident handling. “Monitor risk” is correct because the risk event must be observed, assessed for impact, and tracked as conditions change; this helps determine whether the response is working and whether escalation is needed. “Maintain and initiate incident response plans” is correct because a realized risk often becomes an incident or issue requiring predefined response procedures, assigned responsibilities, communication paths, and containment or recovery actions. Keeping those plans maintained and initiating them promptly supports timely, consistent handling. “Communicate lessons learned from risk events” is also correct because post-event learning is a key part of improving risk response capability; sharing what happened, what worked, and what should change strengthens future controls, response plans, and organizational resilience. This aligns with ISACA’s CRISC focus on identifying, assessing, responding to, and monitoring enterprise IT risk, as described on the ISACA CRISC certification page. It is also consistent with widely accepted incident handling practices, where preparation, detection, response, and post-incident activity are part of the incident response life cycle, as outlined in NIST SP 800-61 Revision 2.

QUESTION NO: 81

The FIRST step for a startup company when developing a disaster recovery plan (DRP) should be to identify:

A. Current vulnerabilities

B. Recovery time objectives (RTOs)

C. Critical business processes

D. A suitable alternate site

ANSWER: C

Explanation:

Critical business processes is correct because disaster recovery planning must begin with understanding what the organization most needs to restore to survive and continue operating. For a startup, resources are often limited, so the DRP should be driven by business priorities rather than by technology assumptions or predefined recovery solutions. Identifying critical business processes establishes the foundation for a business impact analysis, which then supports decisions about acceptable downtime, recovery priorities, required systems, data dependencies, staffing needs and continuity strategies. Once the organization knows which processes are essential, it can define recovery time objectives, recovery point objectives and practical recovery arrangements that align with business risk appetite and operational impact. This sequence is consistent with ISACA’s CRISC focus on risk response, continuity and resilience planning, where risk treatment and recovery activities should be tied to business impact and priority. It also aligns with widely accepted contingency planning guidance, such as NIST SP 800-34, which emphasizes business impact analysis as a key step for identifying and prioritizing mission/business processes and supporting resources. See the ISACA CRISC Exam Content Outline and NIST SP 800-34 Rev. 1.

QUESTION NO: 82

You are the project manager of GHT project. You have initiated the project and conducted the feasibility study. What result would you get after conducting feasibility study?

Each correct answer represents a complete solution. (Choose two.)

A. Recommend alternatives and course of action

B. Risk response plan

C. Project management plan

D. Results of criteria analyzed, like costs, benefits, risk, resources required and organizational impact

ANSWER: A D

Explanation:

A feasibility study is performed early to determine whether a proposed initiative is practical, beneficial and worth pursuing before committing significant resources. The expected output is a structured assessment of the major evaluation criteria, including costs, expected benefits, key risks, resource needs and organizational impact. Therefore, “Results of criteria analyzed, like costs, benefits, risk, resources required and organizational impact” is correct because it reflects the evidence gathered and analyzed to support a go/no-go or selection decision. “Recommend alternatives and course of action” is also correct because a feasibility study should not merely describe the situation; it should compare viable alternatives and recommend the most suitable path forward based on the analysis. This aligns with common project governance practice, where feasibility and business case work support investment decisions through cost-benefit analysis, alternatives evaluation and justification for the selected approach. PMI discusses how a business case and feasibility-related analysis help justify a project and guide the decision to proceed: PMI - Business Case. ISACA also emphasizes governance and value-based decision making for enterprise initiatives: ISACA COBIT resources.

QUESTION NO: 83

A risk practitioner has reviewed new international regulations and realizes the new regulations will affect the organization. Which of the following should be the risk practitioner ' s NEXT course of

action?

A. Conduct a peer response assessment.

B. Update risk scenarios in the risk register.

C. Reevaluate the risk management program.

D. Ensure applications are compliant.

ANSWER: B

Explanation:

Update risk scenarios in the risk register is the correct next action because the practitioner has identified a change in the external business and regulatory environment that may alter the organization’s risk exposure. In CRISC practice, risk scenarios are used to describe how a threat or event could affect business objectives, including regulatory, legal, operational and technology impacts. Once new regulations are known to affect the organization, the risk information should be captured or revised in the risk register so it can be assessed consistently for likelihood, impact, ownership, response and monitoring. This creates an auditable basis for prioritization and later decisions, such as remediation, compliance activities or control changes. ISACA emphasizes the practical use of risk scenarios for understanding and communicating IT risk in business terms, and risk management frameworks also expect organizations to monitor changes that may affect risk posture. See ISACA’s discussion of using risk scenarios to manage IT risk and NIST’s overview of the Risk Management Framework.

QUESTION NO: 84

Which of the following are external risk factors?

Each correct answer represents a complete solution. (Choose three.)

A. Geopolitical situation

B. Complexity of the enterprise

C. Market

D. Competition

ANSWER: A C D

Explanation:

Geopolitical situation, Market, and Competition are external risk factors because they originate outside the enterprise and are largely influenced by forces beyond direct management control. In CRISC-style risk analysis, external factors are part of the organization's external context: political stability, international relations, sanctions, regional conflict, trade restrictions, economic conditions, customer demand, industry trends, supplier conditions, and competitor behavior can all materially affect enterprise objectives and information systems risk. These factors may change the likelihood or impact of risk scenarios, influence control priorities, and affect risk appetite decisions. For example, geopolitical instability can disrupt operations or supply chains, market shifts can change business viability or technology demand, and competition can drive pressure to adopt new digital services quickly, potentially increasing operational or technology risk exposure. This aligns with recognized enterprise risk management practice, which emphasizes understanding the external environment when identifying and assessing risk. See ISACA's risk and governance resources at ISACA IT Risk and NIST guidance on risk assessments, which considers external threat sources and organizational context, at NIST SP 800-30 Revision 1.

QUESTION NO: 85

Which of the following provides the MOST insight into an organization ' s IT threat exposure?

A. Industry benchmarks

B. Risk assessment reports

C. External audit results

D. Tabletop exercises

ANSWER: B

Explanation:

Risk assessment reports provide the most insight into an organization's IT threat exposure because they are developed from the organization's actual environment, assets, vulnerabilities, threat sources, existing controls, and business impact context. In CRISC-aligned risk management, the most useful view of exposure is not a generic comparison or isolated test result, but a structured assessment that connects threats to the organization's specific risk scenarios and evaluates likelihood and impact. This gives management a clearer basis for prioritizing treatment, allocating resources, and deciding whether risk is within tolerance. Risk assessment reports are also typically updated as the threat landscape, control environment, and business processes change, making them a practical source for understanding current exposure. ISACA's CRISC certification emphasizes identifying, assessing, evaluating, and responding to IT risk in support of enterprise objectives, which aligns directly with the purpose of risk assessment reporting. NIST similarly describes risk assessment as the process of identifying threats, vulnerabilities, likelihood, and impact to inform risk decisions. References: ISACA CRISC and NIST SP 800-30 Rev. 1.

QUESTION NO: 86

Which of the following come under the phases of risk identification and evaluation?

Each correct answer represents a complete solution. (Choose three.)

A. Maintain a risk profile

B. Collecting data

C. Analyzing risk

D. Applying controls

ANSWER: A B C

Explanation:

Maintain a risk profile, Collecting data, and Analyzing risk are the activities that align with risk identification and evaluation in ISACA-oriented risk management practice. Collecting data is fundamental because risk identification depends on reliable information about business processes, assets, threats, vulnerabilities, past events, control conditions, and external factors. Without this input, the organization cannot build meaningful risk scenarios or understand where uncertainty may affect business objectives. Analyzing risk is also part of evaluation because the organization must estimate likelihood, impact, business relevance, and other factors to support risk-based decision-making. Maintaining a risk profile completes this set because identified and evaluated risks must be recorded and kept current, including their attributes, ownership, status, and relationship to business services and controls. This enables ongoing visibility, monitoring, and reporting over time. These concepts are consistent with the CRISC focus on IT risk identification, assessment, evaluation, response, and reporting as described by ISACA's CRISC credential information at ISACA CRISC. They also align with widely accepted risk assessment guidance, such as NIST's description of risk assessment as identifying threats and vulnerabilities and determining risk to organizational operations at NIST SP 800-30 Revision 1.

QUESTION NO: 87

An organization has opened a subsidiary in a foreign country. Which of the following would be the BEST way to measure the effectiveness of the subsidiary ' s IT systems controls?

A. Implement IT systems in alignment with business objectives.

B. Review metrics and key performance indicators (KPIs).

C. Review design documentation of IT systems.

D. Evaluate compliance with legal and regulatory requirements.

ANSWER: B

Explanation:

Review metrics and key performance indicators (KPIs) is correct because control effectiveness is best demonstrated through objective, repeatable evidence of how controls are operating over time. In a newly established foreign subsidiary, management needs visibility into whether IT controls are achieving intended outcomes, such as availability, incident response performance, access review completion, vulnerability remediation, backup success, change success rates, and policy exception trends. Well-defined metrics and KPIs enable the parent organization to compare performance against agreed thresholds, risk appetite, service objectives, and control requirements, while also identifying areas requiring corrective action. This aligns with ISACA and COBIT principles that governance and management objectives should be monitored through performance measures and continual improvement mechanisms. Metrics provide more than a point-in-time view; they support ongoing monitoring, trend analysis, and management reporting, which are essential for determining whether controls remain effective in the subsidiary's operational and regulatory environment. For related guidance, see ISACA's COBIT resources at ISACA COBIT and NIST guidance on information security performance measurement at NIST SP 800-55 Rev. 1.

QUESTION NO: 88

While developing obscure risk scenarios, what are the requirements of the enterprise?

Each correct answer represents a part of the solution. (Choose two.)

A. Have capability to cure the risk events

B. Have capability to recognize an observed event as something wrong

C. Have sufficient number of analyst

D. Be in a position that it can observe anything going wrong

ANSWER: B D

Explanation:

Developing obscure risk scenarios requires the enterprise to think beyond events that have already happened and consider low-frequency, emerging, or previously unrecognized conditions. “Be in a position that it can observe anything going wrong” is correct because obscure scenarios depend first on visibility: the organization must have enough monitoring, environmental awareness, stakeholder input, threat intelligence, process knowledge, and operational transparency to notice weak signals or unusual conditions. Without visibility, unusual risk indicators remain hidden and cannot be converted into useful scenarios.

“Have capability to recognize an observed event as something wrong” is also correct because observation alone is not enough. The enterprise must be able to interpret what it sees, distinguish normal variation from abnormal behavior, and connect unusual observations to potential business impact. This recognition capability helps turn vague or rare events into meaningful risk scenarios that can be assessed, communicated, and treated. This aligns with ISACA’s risk-management emphasis on identifying and analyzing IT-related risk in business context, as reflected in the CRISC certification body of knowledge. It is also consistent with risk assessment practices described by NIST, where organizations identify threat events, vulnerabilities, predisposing conditions, likelihood, and impact as part of structured risk analysis: NIST SP 800-30 Rev. 1.

QUESTION NO: 89

Which of the following will BEST help to ensure key risk indicators (KRIs) provide value to risk owners?

A. Ongoing training

B. Timely notification

C. Return on investment (ROI)

D. Cost minimization

ANSWER: B

Explanation:

Timely notification is correct because key risk indicators are most valuable when they enable risk owners to take prompt, informed action before a risk exceeds tolerance or causes material impact. A KRI is not merely a metric for historical reporting; it is an early-warning signal tied to risk appetite, thresholds, and escalation criteria. If the relevant risk owner receives notification at the right time, the owner can investigate the condition, trigger a response plan, adjust controls, or escalate the issue to governance bodies as needed. This aligns with ISACA’s emphasis on risk monitoring and communication as core parts of effective enterprise risk and information systems control practices. ISACA’s Risk IT guidance highlights the importance of risk indicators and reporting to support decision-making and response; see ISACA Journal: The Risk IT Framework. Similarly, NIST describes continuous monitoring as useful when information is reported to support ongoing risk-based decisions; see NIST SP 800-137. Therefore, timely notification best ensures KRIs deliver practical value to risk owners.

QUESTION NO: 90

Which of the following is the FOREMOST root cause of project risk? Each correct answer represents a complete solution. (Choose two.)

A. New system is not meeting the user business needs

B. Delay in arrival of resources

C. Lack of discipline in managing the software development process

D. Selection of unsuitable project methodology

ANSWER: C D

Explanation:

The correct answers are **Lack of discipline in managing the software development process** and **Selection of unsuitable project methodology**. In ISACA-aligned risk thinking, project risk is driven heavily by weaknesses in governance, process control, planning, and execution discipline. A lack of discipline in managing the software development process creates uncertainty in requirements, design, coding, testing, change control, quality assurance, and progress monitoring. When these activities are not consistently controlled, the project is more likely to experience cost overruns, schedule slippage, quality defects, and failure to deliver expected outcomes.

Selection of unsuitable project methodology is also a foremost root cause because the development approach must fit the nature, complexity, volatility, and assurance needs of the system being built. For example, using a rigid approach where requirements are highly uncertain, or using an informal approach for a high-control regulated system, can directly increase delivery and control risk. ISACA's risk guidance emphasizes aligning risk responses and controls with business objectives and context; similarly, project methodology must be aligned to the project environment. See ISACA's overview of IT risk and PMI's discussion of tailoring delivery approaches in project management methodologies.

QUESTION NO: 91

A control owner responsible for the access management process has developed a machine learning model to automatically identify excessive access privileges. What is the risk practitioner ' s BEST course of action?

A. Review the design of the machine learning model against control objectives.

B. Adopt the machine learning model as a replacement for current manual access reviews.

C. Ensure the model assists in meeting regulatory requirements for access controls.

D. Discourage the use of emerging technologies in key processes.

ANSWER: A

Explanation:

Review the design of the machine learning model against control objectives is the best course of action because a risk practitioner should first determine whether the proposed control mechanism is appropriately designed to address the intended risk and support the access management objective. In this case, the objective is to identify excessive access privileges, which directly relates to least privilege, segregation of duties, and timely detection of inappropriate access. A design review allows the practitioner to assess whether the model's data sources, assumptions, decision logic, thresholds, outputs, monitoring approach, and governance are sufficient to produce reliable control evidence. This is especially important because machine learning introduces additional model risk, including data quality issues, drift, lack of explainability, and inconsistent performance over time. ISACA's CRISC exam content emphasizes risk response, control design, and monitoring of risk and control performance as core practitioner responsibilities; see the ISACA CRISC Exam Content Outline. In addition, the NIST AI Risk Management Framework reinforces the need to govern, map, measure, and manage AI-related risks. Therefore, validating the model's design against defined control objectives is the most risk-aware and governance-aligned action before relying on it operationally.

QUESTION NO: 92

Which of the following is MOST helpful in preventing risk events from materializing?

A. Prioritizing and tracking issues

B. Establishing key risk indicators (KRIs)

C. Reviewing and analyzing security incidents

D. Maintaining the risk register

ANSWER: B

Explanation:

Establishing key risk indicators (KRIs) is the most helpful activity for preventing risk events from materializing because KRIs are designed to provide early warning that risk exposure is increasing or that conditions are approaching defined risk thresholds. In CRISC-aligned risk management, prevention depends on detecting changes in the risk environment before they become realized events. Well-defined KRIs are linked to specific risks, monitored against thresholds, and escalated when trends indicate that action is needed. This allows management and risk owners to adjust controls, reduce exposure, or initiate response plans before the risk turns into an incident or issue. KRIs are therefore a proactive risk monitoring mechanism, not merely a recordkeeping or post-event analysis activity. ISACA describes key risk indicators as metrics capable of showing that an enterprise is subject to, or has a high probability of being subject to, risk exceeding the defined risk appetite; see the ISACA Glossary. Similar guidance on using measures to support ongoing monitoring can be found in NIST SP 800-55 Rev. 1.

QUESTION NO: 93

Which of the following role carriers are responsible for setting up the risk governance process, establishing and maintaining a common risk view, making risk-aware business decisions, and setting the enterprise's risk culture?

Each correct answer represents a complete solution. (Choose two.)

A. Senior management

B. Chief financial officer (CFO)

C. Human resources (HR)

D. Board of directors

ANSWER: A D

Explanation:

Senior management and Board of directors are correct because enterprise risk governance is a top-level accountability. In ISACA-aligned governance thinking, the governing body is responsible for ensuring that risk appetite, risk oversight, and governance structures are established and aligned with enterprise objectives. The board sets direction, approves or endorses risk appetite, oversees whether risk is being managed within acceptable limits, and helps shape the tone at the top for risk culture. Senior management translates that direction into operational governance practices by embedding risk-aware decision-making into strategy execution, processes, performance management, and resource allocation. Together, these role carriers establish and maintain a shared enterprise view of risk so that business decisions are made consistently and in line with stakeholder expectations. This division of responsibility is consistent with COBIT's distinction between governance, which evaluates stakeholder needs and sets direction, and management, which plans, builds, runs, and monitors activities to achieve enterprise objectives. See ISACA's COBIT overview at ISACA COBIT and ISACA's CRISC certification domain emphasis on governance and risk management at ISACA CRISC.

QUESTION NO: 94

When using a third party to perform penetration testing, which of the following is the MOST important control to minimize operational impact?

A. Require the vendor to have liability insurance.

B. Perform a background check on the vendor.

C. Require the vendor to sign a nondisclosure agreement.

D. Clearly define the project scope.

ANSWER: D

Explanation:

Clearly define the project scope is correct because the scope establishes the authorized boundaries, timing, targets, testing techniques, escalation paths, and constraints for the penetration test. Penetration testing can affect live systems if activities such as scanning, exploitation attempts, denial-of-service simulation, or social engineering are performed without clear limits. A well-defined scope and rules of engagement help ensure the third party tests only approved systems, avoids sensitive production windows, uses agreed methods, and stops or escalates if unexpected service degradation occurs. This is the control most directly tied to minimizing operational impact because it governs how the testing is executed in the environment. NIST guidance emphasizes that security testing should include careful planning, coordination, and defined rules to reduce adverse effects on operations; see NIST SP 800-115. Similarly, penetration testing standards highlight scoping and pre-engagement interactions as foundational to setting expectations and boundaries before testing begins; see the Penetration Testing Execution Standard.

QUESTION NO: 95

Which of the following is true for risk management frameworks, standards and practices?

Each correct answer represents a part of the solution. (Choose three.)

A. They act as a guide to focus efforts of variant teams.

B. They result in increase in cost of training, operation and performance improvement.

C. They provide a systematic view of "things to be considered" that could harm clients or an enterprise.

D. They assist in achieving business objectives quickly and easily.

ANSWER: A C D

Explanation:

Risk management frameworks, standards and practices are valuable because they create structure, consistency and shared direction for risk-related work across the enterprise. “They act as a guide to focus efforts of variant teams” is correct because a framework gives different business, IT, security, compliance and assurance teams a common approach and vocabulary, helping them align activities with enterprise objectives. “They provide a systematic view of "things to be considered" that could harm clients or an enterprise” is also correct because frameworks help identify, assess and respond to risk in a disciplined way rather than relying on ad hoc judgment. “They assist in achieving business objectives quickly and easily” is correct in the sense that good practices support better prioritization, clearer accountability and more efficient decision-making, allowing the organization to pursue objectives while staying within risk appetite. ISACA’s COBIT materials emphasize governance and management objectives that help enterprises create value while balancing benefits, risk and resources; see ISACA COBIT. Similarly, ISO 31000 describes risk management principles and guidelines that support structured, integrated and effective management of uncertainty; see ISO 31000 Risk Management.

QUESTION NO: 96

A risk practitioner’s PRIMARY focus when validating a risk response action plan should be that risk response:

A. advances business objectives.

B. quantifies risk impact.

C. reduces risk to an acceptable level.

D. aligns with business strategy.

ANSWER: C

Explanation:

The correct answer is **reduces risk to an acceptable level.** In CRISC terms, a risk response action plan is validated to confirm that the selected response will effectively treat the identified risk and bring residual risk within the organization’s risk appetite or tolerance. The risk practitioner’s role is not merely to confirm that the plan is strategically sensible, but to ensure

the response is fit for purpose: the planned actions should measurably address the risk scenario and result in a level of remaining exposure that management is willing to accept. This is central to risk response and mitigation activities in ISACA's CRISC domain structure, where risk treatment decisions are tied to business risk appetite, residual risk, and ongoing monitoring. ISACA's CRISC exam content outline emphasizes governance, risk response, and reporting practices that support enterprise objectives while managing risk exposure appropriately; see the ISACA CRISC Exam Content Outline. ISACA's IT risk resources similarly frame risk response as selecting and implementing measures that keep IT-related risk within acceptable bounds; see ISACA IT Risk Resources.

QUESTION NO: 97

You are the project manager for TTP project. You are in the Identify Risks process. You have to create the risk register. Which of the following are included in the risk register?

Each correct answer represents a complete solution. (Choose two.)

A. List of potential responses

B. List of key stakeholders

C. List of mitigation techniques

D. List of identified risks

ANSWER: A D

Explanation:

List of potential responses and List of identified risks are correct because, during the Identify Risks process, the initial risk register is created to capture the risks that have been discovered and any early response ideas that arise while those risks are being discussed. At this stage, the register is primarily an organized record of known uncertainty: what the risk event is, possible causes, and the potential effect on project objectives such as scope, schedule, cost, quality, or business value. Capturing the List of identified risks is essential because it becomes the foundation for later qualitative analysis, quantitative analysis, response planning, monitoring, and reporting. Capturing the List of potential responses is also appropriate because risk identification workshops, interviews, checklists, and expert judgment often reveal practical response ideas before formal risk response planning begins. Those early ideas are not necessarily final approved treatment plans, but they are useful inputs for later analysis and planning. This aligns with standard project risk management practice described by the Project Management Institute and with risk governance concepts used in ISACA guidance, where risk information must be recorded and maintained to support analysis, response, and monitoring; see the ISACA Glossary.

QUESTION NO: 98

Which of the following are risk components of the COSO ERM framework?

Each correct answer represents a complete solution. (Choose three.)

A. Risk response

B. Internal environment

C. Business continuity

D. Control activities

ANSWER: A B D

Explanation:

Risk response, Internal environment, and Control activities are components of the original COSO Enterprise Risk Management—Integrated Framework that is commonly referenced in CRISC risk governance and control discussions. Internal environment is foundational because it establishes the organization's risk management philosophy, risk appetite, ethical values, governance tone, and overall context for how risk is understood and managed. Risk response is also a core

component because COSO ERM requires management to select appropriate responses to assessed risks, such as avoiding, accepting, reducing, or sharing risk, in alignment with risk appetite and business objectives. Control activities are included because they represent the policies, procedures, and mechanisms that help ensure selected risk responses are carried out effectively across the organization. Together, these components support the broader ERM cycle by connecting governance context, risk decision-making, and execution of controls. COSO's ERM materials describe the framework as a structured approach for managing enterprise risk in relation to strategy and performance; see the COSO ERM Framework. ISACA's CRISC certification domain also emphasizes identifying, assessing, responding to, and monitoring IT and enterprise risk; see ISACA CRISC.

QUESTION NO: 99

What are the PRIMARY objectives of a control?

A. Detect, recover, and attack

B. Prevent, respond, and log

C. Prevent, control, and attack

D. Prevent, recover, and detect

ANSWER: D

Explanation:

Prevent, recover, and detect is correct because controls are implemented to provide reasonable assurance that organizational objectives are achieved and that undesired events are handled appropriately. In a risk and control context, preventive controls are designed to stop an unwanted event before it occurs, such as access restrictions, segregation of duties, or configuration hardening. Detective controls identify that an event, error, exception, or security incident has occurred, enabling management to take timely action; examples include monitoring, logging review, reconciliation, and intrusion detection. Recovery-oriented controls support restoration of services, processes, or data after a disruption or incident, helping the organization return to an acceptable operating state and limit business impact. Together, these objectives align with the practical control lifecycle used in information systems risk management: reduce the likelihood of adverse events, identify events that bypass prevention, and restore operations when impact occurs. This is consistent with widely accepted control guidance, including ISACA's governance and control terminology in the ISACA Glossary and the control objectives reflected in NIST guidance such as NIST SP 800-53 Rev. 5.

QUESTION NO: 100

Which of the following is a risk practitioner's BEST recommendation regarding disaster recovery management (DRM) for Software as a Service (SaaS) providers?

A. Conduct inoremental backups of data in the SaaS environment to a local data center.

B. Implement segregation of duties between multiple SaaS solution providers.

C. Codify availability requirements in the SaaS provider's contract.

D. Conduct performance benchmarking against other SaaS service providers.

ANSWER: C

Explanation:

Codify availability requirements in the SaaS provider's contract is the best recommendation because, in a SaaS model, the customer typically has limited direct control over the provider's underlying infrastructure, backup architecture, failover capabilities, and recovery procedures. A risk practitioner should therefore ensure that disaster recovery expectations are formally defined in the contract and service-level agreement, including measurable commitments such as availability targets, recovery time objectives, recovery point objectives, incident communication timelines, testing expectations, reporting rights, and remedies for nonperformance. This approach aligns risk ownership and accountability with the party operating the

service and gives the organization an enforceable basis for monitoring whether the SaaS provider can support business continuity needs. NIST guidance on cloud computing emphasizes that service agreements should clearly define responsibilities, service levels, continuity expectations, and security obligations for cloud services. ISACA guidance on third-party risk management similarly stresses that organizations should manage supplier risk through contract terms, assurance, and ongoing oversight. See NIST SP 800-146 and ISACA Journal: Third-Party Risk Management.

QUESTION NO: 101

Which of the following events refer to loss of integrity?

Each correct answer represents a complete solution. (Choose three.)

A. Someone sees company's secret formula

B. Someone makes unauthorized changes to a Web site

C. An e-mail message is modified in transit

D. A virus infects a file

ANSWER: B C D

Explanation:

Integrity in information security means information and systems remain accurate, complete, and protected from unauthorized or improper modification. “Someone makes unauthorized changes to a Web site” is a loss of integrity because the trusted state of the website has been altered without authorization, making the published content or configuration unreliable. “An e-mail message is modified in transit” is also a direct integrity failure because the message received is no longer the same as the message originally sent; the data has been changed while moving between sender and recipient. “A virus infects a file” represents loss of integrity because malware can alter file contents, metadata, behavior, or executable code, causing the file to differ from its intended and trusted form. These examples align with the integrity component of the CIA triad, which focuses on preventing unauthorized alteration and ensuring data accuracy and trustworthiness. ISACA’s risk and control guidance treats integrity as a core information criterion, while common security references describe integrity controls as mechanisms that protect data from unauthorized changes. See ISACA’s overview of information and technology risk at ISACA IT Risk and NIST’s definition of integrity at NIST CSRC Glossary: Integrity.

QUESTION NO: 102

In which of the following conditions business units tend to point the finger at IT when projects are not delivered on time?

A. Threat identification in project

B. System failure

C. Misalignment between real risk appetite and translation into policies

D. Existence of a blame culture

ANSWER: D

Explanation:

Existence of a blame culture is correct because this describes an organizational environment where accountability for project outcomes is shifted to another group rather than managed as a shared responsibility. In IT-enabled business projects, success depends on business units clearly defining requirements, participating in prioritization, validating deliverables, and accepting ownership of business outcomes. When a blame culture exists, late delivery or unmet expectations are often attributed to IT alone, even when the underlying causes include unclear requirements, weak sponsorship, inadequate user involvement, or changing business priorities. From a CRISC perspective, this is an important risk culture issue: effective risk management depends on transparent communication, collaborative decision-making, and clear ownership of risk and control responsibilities. A culture that encourages fault-finding instead of shared learning reduces openness and can prevent teams

from identifying and addressing project risks early. ISACA emphasizes the importance of risk culture in how risks are perceived, communicated, and acted upon; see this ISACA Journal article on risk culture. ISACA's COBIT resources also reinforce governance practices that rely on stakeholder engagement and clear accountability.

QUESTION NO: 103

Which of the following BEST enables effective IT control implementation?

A. Key risk indicators (KRIs)

B. Documented procedures

C. Information security policies

D. Information security standards

ANSWER: B

Explanation:

Documented procedures are the best enabler of effective IT control implementation because they translate control intent into repeatable, operational steps. In a risk and control environment, controls are only effective when personnel know exactly what must be done, when it must be done, who is responsible, what evidence must be retained, and how exceptions should be handled. Documented procedures provide that practical execution layer, helping ensure consistency, accountability, training, monitoring, and auditability across business and IT processes. This aligns with control implementation good practice: governance frameworks define objectives and requirements, but procedures make those requirements actionable in day-to-day operations. ISACA's COBIT materials emphasize the importance of managed processes, practices, activities, and work products to achieve governance and management objectives; documented procedures support this by standardizing how control activities are performed. NIST guidance similarly recognizes procedures as the detailed instructions used to implement policies and requirements in operational settings. See ISACA COBIT and NIST SP 800-12 Rev. 1.

QUESTION NO: 104

Which of the following should be the GREATEST concern to a risk practitioner when process documentation is incomplete?

A. Inability to allocate resources efficiently

B. Inability to identify the risk owner

C. Inability to complete the risk register

D. Inability to identify process experts

ANSWER: B

Explanation:

Inability to identify the risk owner is the greatest concern because effective risk management depends on clear accountability. A risk practitioner can document issues, facilitate analysis, and recommend responses, but each material risk must have an accountable owner who understands the business process, accepts responsibility for decisions, and ensures the agreed response is implemented and monitored. When process documentation is incomplete, roles, handoffs, control responsibilities, and decision authority may be unclear, making it difficult to determine who is actually accountable for the risk associated with that process. This directly weakens governance because risks without owners tend to remain unresolved, responses may not be funded or executed, and monitoring becomes ineffective. ISACA's risk guidance emphasizes governance, ownership, and accountability as core elements of managing information and technology risk; see ISACA's IT risk resources at ISACA IT Risk. This is also consistent with widely used risk management practices that assign responsibility for managing identified risks and responses, such as the accountability concepts in NIST risk management guidance at NIST Risk Management.

QUESTION NO: 105

Who should have the authority to approve an exception to a control?

A. information security manager

B. Control owner

C. Risk owner

D. Risk manager

ANSWER: C

Explanation:

Risk owner is correct because approving a control exception is ultimately a risk acceptance decision. When a required control is not implemented, is bypassed, or operates below the required standard, the organization is choosing to tolerate the resulting exposure for a defined business reason, scope and period. The person with accountability for that exposure must therefore approve the exception, since that person is responsible for ensuring the risk remains within the organization's risk appetite and that any compensating measures, expiration dates and follow-up actions are appropriate. This aligns with ISACA's risk governance view that risk decisions should be owned by the accountable business party rather than treated purely as a technical or administrative approval. A risk owner has the authority to balance business value, operational need and residual risk, and to formally accept the consequences of the exception. For related ISACA terminology and governance context, see the ISACA Glossary and ISACA's COBIT governance resources at ISACA COBIT.

QUESTION NO: 106

Which of the following would be the result of a significant increase in the motivation of a malicious threat actor?

A. Increase in mitigating control costs

B. Increase in risk event impact

C. Increase in risk event likelihood

D. Increase in cybersecurity premium

ANSWER: C

Explanation:

Increase in risk event likelihood is correct because motivation is a key factor in determining how probable it is that a threat actor will attempt to exploit a vulnerability. In information risk analysis, likelihood reflects the chance that a threat event will occur, considering factors such as threat capability, intent, targeting, opportunity and frequency. When a malicious actor becomes more motivated, the actor is more likely to initiate attacks, persist longer, invest more effort, or seek additional ways to compromise the target environment. This directly raises the probability of a risk event occurring, even if the potential impact of the event remains unchanged. This aligns with common risk assessment practice, where risk is generally evaluated as a combination of likelihood and impact, and threat-source characteristics such as intent and capability influence likelihood. NIST SP 800-30 describes threat event likelihood in relation to threat sources and their characteristics, including adversarial intent and capability: NIST SP 800-30 Rev. 1. ISACA's risk and control guidance similarly treats risk assessment as a structured evaluation of threat scenarios, likelihood and business impact: ISACA Glossary.

QUESTION NO: 107

Reviewing historical risk events is MOST useful in which of the following phases of the risk management life cycle?

A. Risk reporting

B. Risk identification

C. Risk mitigation

D. Risk monitoring

ANSWER: B

Explanation:

Risk identification is correct because historical risk events provide one of the strongest practical inputs for recognizing relevant risk scenarios, threat patterns, control weaknesses, root causes, and business impacts that may recur. In the risk management life cycle, identification is the phase where the organization determines what could affect objectives, assets, processes, systems, or services. Prior incidents, near misses, audit findings, loss events, external breaches, and industry events help risk practitioners move beyond theoretical risk lists and build scenarios that reflect actual conditions and trends. This aligns with CRISC-oriented practice, where risk identification should be informed by organizational context, past events, and available risk-related data so that risks can be assessed and treated appropriately later in the process. ISACA's IT risk guidance emphasizes understanding and managing technology-related risk in relation to enterprise objectives, which depends on first identifying meaningful risk scenarios. See ISACA's overview of IT risk at ISACA IT Risk and ISACA's CRISC certification information at ISACA CRISC.

QUESTION NO: 108

Jeff works as a Project Manager for www.company.com Inc. He and his team members are involved in the identify risk process. Which of the following tools & techniques will Jeff use in the identify risk process?

Each correct answer represents a complete solution. (Choose three.)

A. Information gathering technique

B. Documentation reviews

C. Checklist analysis

D. Risk categorization

ANSWER: A B C

Explanation:

Information gathering technique, Documentation reviews, and Checklist analysis are correct because they are recognized tools and techniques used during the project risk identification process. In project risk management, the purpose of identifying risks is to systematically discover uncertain events or conditions that could affect objectives and to document their characteristics for later analysis and response planning. Information gathering technique supports this by using structured approaches such as brainstorming, interviews, and facilitated sessions to draw out risk knowledge from stakeholders and subject matter experts. Documentation reviews are also central because project plans, assumptions, contracts, requirements, estimates, and historical records often reveal inconsistencies, gaps, or uncertainty that can become risk sources. Checklist analysis is useful because it leverages prior experience, organizational process assets, lessons learned, and known risk categories to prompt the team to consider common risks that might otherwise be missed. These techniques align with the established project risk management practices described in PMI guidance, including the PMBOK framework, and with broader risk assessment principles that emphasize structured identification based on evidence, expert input, and prior knowledge. See PMI's overview of its foundational standards at PMI PMBOK Guide and Standards and NIST's risk assessment guidance at NIST SP 800-30 Rev. 1.

QUESTION NO: 109

Which of the following is the MOST important consideration for protecting data assets m a Business application system?

A. Application controls are aligned with data classification lutes

B. Application users are periodically trained on proper data handling practices

C. Encrypted communication is established between applications and data servers

D. Offsite encrypted backups are automatically created by the application

ANSWER: A

Explanation:

Aligning application controls with data classification rules is the most important consideration because data protection should be risk-based and proportional to the sensitivity, criticality, and regulatory requirements of the information being processed. In a business application, classification provides the foundation for deciding which controls are required, such as access restrictions, logging, retention, encryption, masking, segregation of duties, and approval workflows. Without this alignment, controls may be applied inconsistently, leaving highly sensitive data underprotected or causing unnecessary cost and operational friction for lower-risk data. This approach is consistent with information security governance and risk management practice: first understand the value and sensitivity of the information asset, then design and operate controls that meet the required level of protection. NIST guidance on information categorization similarly emphasizes that security control selection depends on the potential impact associated with the information and system, as described in NIST SP 800-60. ISACA also highlights data classification as a practical basis for applying appropriate handling and protection requirements in Keeping Data Classification Simple.

QUESTION NO: 110

While reviewing an organization's monthly change management metrics, a risk practitioner notes that the number of emergency changes has increased substantially Which of the following would be the BEST approach for the risk practitioner to take?

A. Temporarily suspend emergency changes.

B. Document the control deficiency in the risk register.

C. Conduct a root cause analysis.

D. Continue monitoring change management metrics.

ANSWER: C

Explanation:

Conduct a root cause analysis is the best approach because a substantial increase in emergency changes is a risk indicator that may point to weaknesses in planning, release management, testing, capacity management, incident response, or governance of the change process. For a CRISC practitioner, the priority is to understand the underlying cause of the trend before recommending a risk response or escalating it as a control deficiency. Root cause analysis helps determine whether the increase is due to legitimate business urgency, recurring system instability, inadequate forward scheduling, poor requirements definition, failed normal changes, or misuse of the emergency change path to bypass required controls. Once the cause is understood, management can select an appropriate and proportionate treatment, such as improving change approval criteria, strengthening post-implementation reviews, adjusting resourcing, or addressing technical instability. This aligns with risk management practice because metrics and key risk indicators should trigger analysis that supports informed decision-making, not merely observation. ISACA emphasizes the use of governance, risk, and control practices to support reliable information systems outcomes; see the ISACA Glossary. NIST also highlights the importance of controlled configuration and change management processes in maintaining system security and reliability; see NIST SP 800-128.

QUESTION NO: 111

What are the two MAJOR factors to be considered while deciding risk appetite level? Each correct answer represents a part of the solution. (Choose two.)

A. The amount of loss the enterprise wants to accept

B. Alignment with risk-culture

C. Risk-aware decisions

D. The capacity of the enterprise's objective to absorb loss.

ANSWER: A D

Explanation:

The correct factors are “The amount of loss the enterprise wants to accept” and “The capacity of the enterprise's objective to absorb loss.” In ISACA risk management terminology, risk appetite is the amount and type of risk an enterprise is willing to accept while pursuing its objectives. Setting that level requires both a desire-based view and a capacity-based view. The amount of loss the enterprise wants to accept reflects management’s and the board’s intended tolerance for risk in pursuit of value, including their willingness to accept uncertainty, financial impact, operational disruption, or reputational consequences. The capacity of the enterprise's objective to absorb loss is equally important because risk appetite cannot be set responsibly without understanding how much impact the enterprise can realistically withstand before strategic objectives, solvency, compliance, or stakeholder trust are threatened. Together, these two considerations help ensure risk appetite is not merely aspirational but is grounded in enterprise objectives and practical resilience. ISACA’s glossary defines key risk terms such as risk appetite in the context of enterprise risk governance: ISACA Glossary. COSO’s enterprise risk management guidance also supports linking risk appetite to strategy, objectives, and performance capacity: COSO ERM Guidance.

QUESTION NO: 112

Which of the following are the responsibilities of Enterprise risk committee?

Each correct answer represents a complete solution. (Choose three.)

A. React to risk events

B. Analyze risk

C. Risk aware decision

D. Articulate risk

ANSWER: B C D

Explanation:

The correct responsibilities are **Analyze risk**, **Risk aware decision**, and **Articulate risk**. In ISACA-aligned risk governance, an enterprise risk committee provides executive-level coordination and oversight so that risk information is understood, communicated, and used in decision-making across the enterprise. This includes supporting the analysis of significant risk information so management can understand exposure in relation to business objectives, appetite, and tolerance. It also includes articulating risk clearly to stakeholders, ensuring risk is expressed in business terms and communicated consistently enough for prioritization and escalation. Finally, the committee has a key role in enabling risk-aware decisions, meaning that strategic and operational choices are made with an informed view of risk, expected benefit, and acceptable exposure. ISACA’s risk governance guidance emphasizes integrating risk management with enterprise objectives and decision processes, rather than treating risk as a separate technical activity. Useful references include ISACA’s overview of CRISC and IT risk management and the COSO guidance on enterprise risk management, which aligns with the need for governance bodies to evaluate, communicate, and use risk information in decision-making.

QUESTION NO: 113

You are the project manager of the HJK Project for your organization. You and the project team have created risk responses for many of the risk events in the project. Where should you document the proposed responses and the current status of all identified risks?

A. Stakeholder management strategy

B. Lessons learned documentation

C. Risk register

D. Risk management plan

ANSWER: C

Explanation:

Risk register is correct because it is the central project document used to record identified risks and maintain key information about each risk throughout the risk life cycle. In good risk management practice, the risk register captures the risk description, causes, categories, probability, impact, risk owner, planned or proposed responses, residual risk information, and the current status of each risk. Once risk responses have been developed, they should be added to the risk register so the project team can track accountability, monitor implementation, and keep risk information current as the project changes. This aligns with ISACA-oriented risk practice, where risk documentation should support ongoing monitoring, ownership, treatment decisions, and reporting. It also aligns with common project risk management guidance, which treats the risk register as a living artifact updated as risks are identified, analyzed, responded to, and monitored. See ISACA's risk-related terminology and governance resources at ISACA Glossary and PMI's discussion of project risk management practices at PMI.

QUESTION NO: 114

Which of the following are the security plans adopted by the organization?

Each correct answer represents a complete solution. (Choose three.)

A. Business continuity plan

B. Backup plan

C. Disaster recovery plan

D. Project management plan

ANSWER: A B C

Explanation:

Business continuity plan, Backup plan, and Disaster recovery plan are correct because they are commonly adopted organizational security and resilience plans that help ensure critical business services and information systems can withstand, respond to, and recover from disruptive events. A Business continuity plan focuses on maintaining essential business operations during and after incidents such as cyberattacks, outages, natural disasters, or supplier failures. A Backup plan supports information availability and recoverability by defining what data and systems are backed up, how often backups occur, where they are stored, and how restoration is validated. A Disaster recovery plan provides the technical recovery procedures needed to restore IT infrastructure, applications, data, and services after a significant disruption. Together, these plans support core information security objectives, especially availability and resilience, and align with risk response and continuity practices expected in CRISC-related governance and risk management contexts. NIST guidance on contingency planning describes backup, recovery, and continuity capabilities as key components of effective information system resilience; see NIST SP 800-34 Rev. 1. Business continuity planning is also recognized as a structured way to keep essential functions operating during disruptions, as described by Ready.gov Business Continuity Planning.

QUESTION NO: 115

A key risk indicator (KRI) threshold has reached the alert level, indicating data leakage incidents are highly probable. What should be the risk practitioner ' s FIRST course of action?

A. Update the KRI threshold.

B. Recommend additional controls.

C. Review incident handling procedures.

D. Perform a root cause analysis.

ANSWER: C

Explanation:

Review incident handling procedures is the correct first course of action because an alert-level KRI indicates that risk exposure has moved beyond normal monitoring and the organization should be ready to respond if the risk event materializes. In this situation, the risk practitioner's immediate priority is to confirm that the established response process is current, understood, and actionable. This includes validating escalation paths, roles and responsibilities, communication requirements, evidence handling, containment steps, and reporting expectations for a potential data leakage incident. KRIs are intended to provide early warning so management can take timely action before losses occur or before an incident worsens. Reviewing incident handling procedures aligns with that purpose because it ensures the organization can react quickly and consistently if leakage is detected. Incident response guidance also emphasizes preparation as a core phase of effective incident handling, including maintaining plans, procedures, communication methods, and response capabilities. See ISACA's discussion of key risk indicators in risk management at ISACA Journal and NIST's incident handling guidance at NIST SP 800-61 Rev. 2.

QUESTION NO: 116

Which of the following should be the PRIMARY objective of a risk awareness training program?

A. To promote awareness of the risk governance function.

B. To clarify fundamental risk management principles.

C. To enable risk-based decision making.

D. To ensure sufficient resources are available.

ANSWER: C

Explanation:

To enable risk-based decision making is the correct answer because the main value of risk awareness training is not simply to communicate concepts, structures, or roles, but to influence day-to-day behavior and judgment. In a CRISC context, effective risk awareness helps personnel understand how their actions affect enterprise objectives, how to recognize risk events or control weaknesses, and how to escalate or respond in a way that aligns with the organization's risk appetite and tolerance. The outcome should be that stakeholders make better operational and strategic decisions when faced with uncertainty, trade-offs, control requirements, or competing business priorities.

ISACA's CRISC domains emphasize governance, risk response, reporting, and information systems control as practices that support informed decision-making around IT risk. A risk awareness program should therefore equip employees and stakeholders to apply risk thinking in their specific responsibilities, so risk management becomes embedded in business processes rather than treated as a separate compliance activity. This is consistent with broader risk management guidance, where communication and consultation are used to support sound decisions under uncertainty. See ISACA's CRISC exam content outline at ISACA CRISC Exam Content Outline and ISO's overview of risk management principles at ISO 31000 Risk Management.

QUESTION NO: 117

Which of the following come under the management class of controls?

Each correct answer represents a complete solution. (Choose two.)

A. Risk assessment control

B. Audit and accountability control

C. Program management control

D. Identification and authentication control

ANSWER: A C

Explanation:

Risk assessment control and Program management control are correct because, in the NIST security control structure commonly used for information security and risk-control exam content, security controls are grouped into control families and historically categorized into management, operational, and technical classes. The management class focuses on governance, oversight, planning, risk decision-making, authorization, and organization-wide security program direction rather than hands-on system enforcement. Risk assessment control belongs in this management class because it supports management's responsibility to identify threats, vulnerabilities, likelihood, impact, and overall risk posture so that informed risk responses and control priorities can be established. Program management control also belongs in this class because it addresses organization-level security program governance, including policy, strategy, resources, enterprise risk management coordination, and oversight activities that support the broader control environment. These two areas are management-oriented because they help leadership define, assess, monitor, and steer security and risk activities across systems and business processes. For reference, see the NIST SP 800-53 publication page at NIST SP 800-53 Revision 4 and the current NIST control catalog resources at NIST SP 800-53 Controls.

QUESTION NO: 118

Which of the following would be the GREATEST concern for an IT risk practitioner when an employees.....

A. The organization's structure has not been updated

B. Unnecessary access permissions have not been removed.

C. Company equipment has not been retained by IT

D. Job knowledge was not transferred to employees m the former department

ANSWER: B

Explanation:

Unnecessary access permissions have not been removed. is the correct answer because excessive or outdated access is a direct and immediate information security risk. When an employee changes role, department, responsibility, or employment status, access rights should be reviewed and adjusted promptly according to the principle of least privilege. If legacy permissions remain active, the employee may retain the ability to view, change, approve, or extract information that is no longer required for the current role. From a CRISC perspective, this represents the greatest concern because it increases the likelihood and potential impact of unauthorized access, segregation-of-duties conflicts, fraud, privacy violations, and regulatory noncompliance. Effective identity and access management requires that user privileges be aligned with current business need and that access changes be controlled through formal provisioning and deprovisioning processes. NIST describes account management controls that include disabling, removing, or modifying access when users are transferred or when access is no longer required; see NIST SP 800-53 Rev. 5. ISACA also emphasizes access control and least-privilege concepts in its security and governance guidance, such as ISACA Glossary.

QUESTION NO: 119

Which of tie following is We MOST important consideration when implementing ethical remote work monitoring?

A. Monitoring is only conducted between official hours of business

B. Employees are informed of how they are bong monitored

C. Reporting on nonproductive employees is sent to management on a scheduled basis

D. Multiple data monitoring sources are integrated into security incident response procedures

ANSWER: B

Explanation:

Employees are informed of how they are bong monitored is the correct choice because ethical monitoring depends first on transparency and informed awareness. In a remote work environment, monitoring can involve activity logs, device telemetry, communications metadata, application usage, or productivity-related data. Employees should clearly understand what is collected, why it is collected, how it will be used, who can access it, and how long it will be retained. This supports fairness, privacy expectations, accountability, and trust, which are essential elements of a risk-aware control environment. From an ISACA perspective, professionals are expected to support appropriate governance and act with due care and objectivity; transparent monitoring helps ensure that control activities do not become excessive, hidden, or misaligned with organizational policy. It also aligns with privacy risk management practices promoted by frameworks such as the NIST Privacy Framework, which emphasizes communicating data processing activities and managing privacy risk. For reference, see the ISACA Code of Professional Ethics and the NIST Privacy Framework.

QUESTION NO: 120

Which of the following situations would BEST justify escalation to senior management?

A. Residual risk equals current risk.

B. Residual risk exceeds acceptable limits.

C. Residual risk is inadequately recorded.

D. Residual risk remains after controls have been applied.

ANSWER: B

Explanation:

“Residual risk exceeds acceptable limits” is the best justification for escalation because it indicates that, even after existing controls or planned responses are considered, the remaining exposure is outside the organization’s approved risk appetite or tolerance. In CRISC terms, management must be informed when risk cannot be reduced to an acceptable level by normal control activities, because senior leadership is accountable for deciding whether to accept the risk, fund additional treatment, change business objectives, transfer the exposure, or stop the activity. Escalation is especially appropriate when the decision requires authority beyond the risk owner or control owner, involves trade-offs between cost and business value, or may affect enterprise objectives. ISACA’s risk management guidance emphasizes aligning risk decisions with business objectives and appetite, while NIST similarly describes risk response decisions as management decisions based on organizational risk tolerance. See the ISACA Glossary for risk terminology and NIST SP 800-39 for enterprise risk management concepts related to risk tolerance and response.

QUESTION NO: 121

Which of the following is MOST important to identify when developing generic risk scenarios?

A. The organization’s vision and mission

B. Resources required for risk mitigation

C. Impact to business objectives

D. Risk-related trends within the industry

ANSWER: C

Explanation:

Impact to business objectives is correct because a risk scenario is useful only when it can be tied to what the enterprise is trying to achieve and what could prevent, degrade, or delay those objectives. In ISACA’s risk management view, risk is

evaluated in business terms, so generic scenarios must be made relevant by understanding the potential business consequence: financial loss, operational disruption, regulatory exposure, reputational harm, safety impact, or failure to meet strategic goals. Identifying this impact helps determine whether a scenario is material, how it should be prioritized, and how later analysis should assess likelihood, magnitude, and response. This aligns with the CRISC emphasis on identifying and assessing IT risk in relation to enterprise objectives, rather than treating scenarios as isolated technical events. ISACA's CRISC exam content outline highlights governance and risk assessment activities in the context of organizational objectives, and ISACA's glossary frames risk-related concepts around business impact and objectives. References: ISACA CRISC Exam Content Outline and ISACA Glossary.

QUESTION NO: 122

Which of the following should be considered to ensure that risk responses that are adopted are cost-effective and are aligned with business objectives?

Each correct answer represents a part of the solution. (Choose three.)

A. Identify the risk in business terms

B. Recognize the business risk appetite

C. Adopt only pre-defined risk responses of business

D. Follow an integrated approach in business

ANSWER: A B D

Explanation:

Identify the risk in business terms, Recognize the business risk appetite, and Follow an integrated approach in business are correct because effective risk response selection must connect risk treatment decisions directly to enterprise value, tolerance, and operational context. Identifying the risk in business terms converts technical or control-focused issues into impacts such as financial loss, productivity disruption, regulatory exposure, confidentiality loss, or missed business opportunity. This makes it possible to compare response costs with the value protected and to justify investments through a business case.

Recognizing the business risk appetite is also essential because responses should reduce risk to a level management is willing to accept, not necessarily eliminate risk at any cost. A cost-effective response is one that is proportionate to the organization's tolerance, strategic priorities, and expected benefits. Following an integrated approach in business ensures risk responses are not designed in isolation; they should consider business processes, stakeholders, dependencies, existing controls, and enterprise objectives. This aligns with ISACA's CRISC focus on IT risk identification, assessment, response, and reporting, and with COBIT's emphasis on aligning governance and management practices with enterprise goals and value delivery. See ISACA CRISC and ISACA COBIT.

QUESTION NO: 123

Which of the following BEST describes the utility of a risk?

A. The finance incentive behind the risk

B. The potential opportunity of the risk

C. The mechanics of how a risk works

D. The usefulness of the risk to individuals or groups

ANSWER: D

Explanation:

The usefulness of the risk to individuals or groups is correct because "utility" in risk analysis refers to the perceived value, usefulness, or preference associated with accepting or avoiding a risk. In CRISC-style risk thinking, risk is not viewed only as

something negative; it is considered in relation to business objectives, potential value, and stakeholder appetite. Different individuals or groups may assign different utility to the same risk because their objectives, tolerance, incentives, and expected outcomes differ. For example, a business sponsor may see value in accepting a certain project risk because it enables market growth, while another stakeholder may view the same uncertainty as less useful because it threatens operational stability. This aligns with ISACA's emphasis that risk decisions should support enterprise objectives and be evaluated in terms of business value, risk appetite, and risk response. See ISACA's CRISC overview at ISACA CRISC and ISACA's IT risk resources at ISACA IT Risk.

QUESTION NO: 124

You work as a Project Manager for Company Inc. You have to conduct the risk management activities for a project. Which of the following inputs will you use in the plan risk management process?

Each correct answer represents a complete solution. (Choose three.)

A. Quality management plan

B. Schedule management plan

C. Cost management plan

D. Project scope statement

ANSWER: B C D

Explanation:

Schedule management plan, Cost management plan, and Project scope statement are correct inputs to the plan risk management process under the traditional PMBOK-style project risk management framework. The plan risk management process establishes how risk management activities will be structured, performed, budgeted, timed, and integrated with the overall project management approach. Schedule management plan is relevant because risk planning must account for schedule assumptions, timing of risk reviews, schedule contingency, and how schedule-related uncertainty will be assessed. Cost management plan is also an input because risk management planning must define how contingency reserves, management reserves, and risk-related budget reporting will be handled. Project scope statement is important because it defines project boundaries, deliverables, assumptions, and constraints, which strongly influence the scale and depth of risk management required. Together, these inputs help the project manager tailor risk management to the project's size, complexity, constraints, and stakeholder expectations. This aligns with PMI's project risk management guidance, which emphasizes integrating risk planning with scope, schedule, and cost planning. See PMI's overview of project risk management at PMI and the PMBOK Guide standards page at PMI PMBOK Guide.

QUESTION NO: 125

As part of an overall IT risk management plan, an IT risk register BEST helps management:

A. stay current with existing control status

B. align IT processes with business objectives

C. understand the organizational risk profile

D. communicate the enterprise risk management policy

ANSWER: C

Explanation:

understand the organizational risk profile is correct because an IT risk register is a consolidated record of identified IT-related risks, typically including risk descriptions, likelihood, impact, ownership, response plans, residual risk, and current treatment status. Its main management value is not just tracking individual controls, but providing a structured and current view of the organization's exposure across technology, processes, services, and business objectives. This enables leaders

to see which risks are most significant, compare them against risk appetite and tolerance, prioritize treatment activities, assign accountability, and make informed decisions about resources and governance. In CRISC terms, the risk register supports risk identification, assessment, response, and monitoring by maintaining risk information in a way that can be reviewed and reported to stakeholders. This aligns with ISACA's focus on IT risk as a business issue requiring visibility for decision-making, as reflected in ISACA risk management resources such as ISACA IT Risk. NIST also describes risk assessment outputs as inputs for risk response and ongoing monitoring, which supports the idea that a risk register helps management understand the overall risk posture; see NIST SP 800-30 Rev. 1.

QUESTION NO: 126

Which of the following scenarios is MOST important to consider when assessing data integrity risk?

A. Loss of business due to the lack of data

B. Cost of recreating data

C. Impact of poor data quality on business decision-making

D. Data extract, transform, and load (ETL) costs

ANSWER: C

Explanation:

Impact of poor data quality on business decision-making is the best answer because data integrity risk is primarily about whether information remains accurate, complete, valid and reliable enough to support business processes and decisions. In a CRISC context, risk assessment should focus on business impact, not just technical symptoms or operational costs. If data used by management, customers, regulators or automated processes is inaccurate or inconsistent, the organization may make flawed strategic, financial, operational or compliance decisions. That is the central risk consequence of compromised integrity: trust in information is reduced, and business outcomes can be materially affected. This aligns with the risk-based view used in ISACA guidance, where information quality and integrity are evaluated in terms of enterprise objectives and value delivery. It is also consistent with broader cybersecurity guidance that treats integrity as protection against improper information modification or destruction, including ensuring information authenticity and non-repudiation. See ISACA's overview of COBIT and NIST's definition of integrity in NIST CSRC Glossary.

QUESTION NO: 127

Which of the following is the MOST significant indicator of the need to perform a penetration test?

A. An increase in the number of infrastructure changes

B. An increase in the number of security incidents

C. An increase in the number of high-risk audit findings

D. An increase in the percentage of turnover in IT personnel

ANSWER: B

Explanation:

An increase in the number of security incidents is the strongest indicator that a penetration test may be needed because it provides direct evidence that the organization's environment may be exposed to exploitable weaknesses or that existing controls are not operating effectively against real-world threats. A penetration test is intended to emulate attacker behavior and validate whether vulnerabilities can be exploited to compromise systems, data, or business processes. When incidents are increasing, management needs more than a theoretical assessment of risk; it needs practical assurance about how attackers could gain access, how far they could move, and which control weaknesses require priority remediation. This aligns with ISACA's risk-based view that assurance and testing activities should be driven by threat exposure, control effectiveness, and business risk. NIST similarly describes penetration testing as a method for identifying ways an adversary

could exploit vulnerabilities in systems and networks. See ISACA Journal: Penetration Testing—A Risk-Based Approach and NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.

QUESTION NO: 128

Which of the following is the MOST effective way to help ensure accountability for managing risk?

A. Assign process owners to key risk areas.

B. Obtain independent risk assessments.

C. Assign incident response action plan responsibilities.

D. Create accurate process narratives.

ANSWER: A

Explanation:

Assign process owners to key risk areas is correct because accountability in risk management is strongest when specific individuals or roles are explicitly made responsible for the risks associated with the processes they manage. A process owner has the operational knowledge, authority and day-to-day influence needed to identify risk conditions, evaluate impacts, select appropriate responses, monitor controls and report changes in risk exposure. This creates clear ownership rather than leaving risk management as a general or shared activity with no single accountable party. In ISACA-aligned governance practices, effective risk governance depends on defined roles, responsibilities and decision rights so that risk treatment and monitoring are embedded into business processes. COBIT emphasizes governance and management objectives supported by clear responsibility assignment, while ISACA's CRISC body of knowledge focuses on identifying, assessing, responding to and reporting risk in a way that supports enterprise objectives. Establishing named process owners for key risk areas directly supports those principles by linking risk accountability to the business activities where the risk originates and must be managed. References: ISACA CRISC certification and ISACA COBIT resources.

QUESTION NO: 129

You are the risk professional of your enterprise. You have performed cost and benefit analysis of control that you have adopted. What are all the benefits of performing cost and benefit analysis of control? Each correct answer represents a complete solution. (Choose three.)

A. It helps in determination of the cost of protecting what is important

B. It helps in taking risk response decisions

C. It helps in providing a monetary impact view of risk

D. It helps making smart choices based on potential risk mitigation costs and losses

ANSWER: A C D

Explanation:

Cost and benefit analysis of a control is used to determine whether the value of reducing risk justifies the resources required to implement and operate the control. "It helps in determination of the cost of protecting what is important" is correct because the analysis identifies the financial commitment needed to safeguard critical assets, processes, and information. "It helps in providing a monetary impact view of risk" is also correct because comparing costs and benefits requires risk professionals to translate potential losses, exposure, and mitigation value into business terms that management can understand. "It helps making smart choices based on potential risk mitigation costs and losses" is correct because the result supports rational prioritization: controls should generally be selected when the expected reduction in loss exposure, compliance impact, or business disruption is worth the cost. This aligns with ISACA's risk-management emphasis on business value and informed decision-making, as reflected in the CRISC certification domain focus, and with NIST guidance that risk responses should be considered in light of organizational priorities, resources, and impact, as described in NIST SP 800-30 Rev. 1.

QUESTION NO: 130

Which of the following is a risk practitioner's BEST recommendation to address an organization's need to secure multiple systems with limited IT resources?

A. Apply available security patches.

B. Schedule a penetration test.

C. Conduct a business impact analysis (BIA)

D. Perform a vulnerability analysis.

ANSWER: C

Explanation:

Conduct a business impact analysis (BIA) is the best recommendation because limited IT resources require a risk-based and business-aligned prioritization of systems. A BIA helps the organization identify which business processes, applications, data, and supporting systems are most critical, and it estimates the potential impact if those systems are unavailable, compromised, or degraded. For a CRISC risk practitioner, the key objective is not simply to apply technical activity everywhere, but to guide management toward allocating scarce resources where they reduce the greatest business risk. By understanding criticality and impact, the organization can decide which systems should receive attention first and ensure security investments support business priorities. This aligns with ISACA's risk management focus on business value, risk optimization, and informed decision-making, as reflected in the CRISC certification domain focus. NIST also describes BIA as a process for identifying and prioritizing critical systems and processes based on mission and business impact, which supports effective continuity and protection planning; see NIST SP 800-34 Rev. 1.

QUESTION NO: 131

An organization has determined a risk scenario is outside the defined risk tolerance level. What should be the NEXT course of action?

A. Develop a compensating control

B. Identify risk responses

C. Allocate remediation resources

D. Perform a cost-benefit analysis

ANSWER: B

Explanation:

Identify risk responses is the correct next course of action. In CRISC terms, once a risk scenario has been analyzed and found to exceed the organization's defined risk tolerance, management must determine how the risk should be treated. This means identifying appropriate response options, such as mitigating, avoiding, sharing/transferring, or accepting the risk under formally approved conditions. The key point is that the organization should not immediately jump into implementing a specific control or committing resources until the available response alternatives have been considered and aligned with business objectives, risk appetite, and stakeholder expectations.

ISACA's risk management guidance emphasizes that risk tolerance provides a threshold for deciding when action is required; when exposure is above that threshold, a risk response process should be initiated. The response should be selected based on the nature of the scenario, the desired residual risk level, and the value of the business process or asset affected. For more context, see ISACA's information on risk-related terminology and the Risk IT Framework.

QUESTION NO: 132

Which of the following BEST enables an organization to determine whether risk management is aligned with its goals and objectives?

A. Environmental changes that impact risk are continually evaluated.

B. The organization has approved policies that provide operational boundaries.

C. Organizational controls are in place to effectively manage risk appetite.

D. The organization has an approved enterprise architecture (EA) program.

ANSWER: B

Explanation:

The organization has approved policies that provide operational boundaries is the best answer because approved policies translate governance direction, business objectives, and risk appetite into practical limits for decision-making and operations. In an ISACA-style risk governance context, management needs defined and approved boundaries to judge whether risk identification, assessment, response, and monitoring activities are supporting enterprise goals rather than operating in isolation. These policies create the benchmark against which risk-related decisions can be evaluated: whether risks are being accepted, mitigated, transferred, or avoided consistently with the organization's objectives and authorized tolerance for risk. COBIT emphasizes that governance and management practices should be aligned with stakeholder needs and enterprise goals, and policies are a key mechanism for communicating management intent and expected behavior. Similarly, CRISC focuses on ensuring that IT and enterprise risk are identified and managed in support of business objectives. For more context, see ISACA's overview of COBIT and the CRISC certification, both of which emphasize governance, alignment, and risk management in support of enterprise objectives.

QUESTION NO: 133

You are the project manager of GHT project. A stakeholder of this project requested a change request in this project. What are your responsibilities as the project manager that you should do in order to approve this change request?

Each correct answer represents a complete solution. (Choose two.)

A. Archive copies of all change requests in the project file.

B. Evaluate the change request on behalf of the sponsor

C. Judge the impact of each change request on project activities, schedule and budget.

D. Formally accept the updated project plan

ANSWER: A C

Explanation:

Archive copies of all change requests in the project file and Judge the impact of each change request on project activities, schedule and budget are the correct responsibilities for the project manager in a disciplined change control process. A project manager is accountable for ensuring that every requested change is documented, traceable, and retained with the project records so the organization has an audit trail of what was requested, assessed, approved, deferred, or rejected. This supports governance, accountability, and later review of project decisions. The project manager also has the responsibility to analyze the effect of a proposed change before it is approved, including likely impacts on scope, schedule, cost, resources, quality, risk, and dependent work. Without that impact assessment, the approver cannot make an informed decision about whether the change is beneficial and acceptable. This aligns with recognized project management practice for integrated change control, where change requests are logged, analyzed, and routed through the defined governance process. See PMI's overview of project management standards at PMI PMBOK Guide and Standards and ISACA's CRISC certification context for risk-informed governance and control at ISACA CRISC.

QUESTION NO: 134

While defining the risk management strategies, what are the major parts to be determined first? Each correct answer represents a part of the solution. (Choose two.)

A. IT architecture complexity

B. Organizational objectives

C. Risk tolerance

D. Risk assessment criteria

ANSWER: B C

Explanation:

Organizational objectives and Risk tolerance are correct because an effective risk management strategy must start by understanding what the enterprise is trying to achieve and how much risk it is willing to accept while pursuing those goals. Organizational objectives provide the business context for identifying relevant risk scenarios, prioritizing risk responses, and ensuring that risk decisions support value creation rather than operating as a separate compliance exercise. In ISACA-aligned risk practice, risk management is expected to be business-focused and tied to enterprise goals, which is also reflected in the CRISC emphasis on governance, risk identification, assessment, response, and reporting. Risk tolerance is equally foundational because it defines the acceptable level of variation from expected outcomes. Once tolerance is understood, risk professionals can determine whether risks should be accepted, mitigated, transferred, or avoided based on whether exposure exceeds the organization's agreed boundaries. These two elements establish the framework for later activities such as detailed assessment, control selection, monitoring, and reporting. See ISACA's CRISC overview at ISACA CRISC and ISACA's COBIT resources at ISACA COBIT.

QUESTION NO: 135

What are the steps that are involved in articulating risks? Each correct answer represents a complete solution. (Choose three.)

A. Identify business opportunities.

B. Identify the response

C. Communicate risk analysis results and report risk management activities and the state of compliance.

D. Interpret independent risk assessment findings.

ANSWER: A C D

Explanation:

In ISACA's CRISC context, articulating risk is about translating risk information into business-relevant communication that supports decision-making. "Identify business opportunities." is correct because risk articulation is not limited to negative exposure; it also includes recognizing where risk-aware decisions can create value or enable business objectives. "Communicate risk analysis results and report risk management activities and the state of compliance." is correct because risk analysis must be expressed clearly to stakeholders, including the current status of risk treatment, control performance, and compliance posture. "Interpret independent risk assessment findings." is also correct because independent assessments provide objective input that must be understood, contextualized, and communicated in terms that management can use. Together, these activities align with CRISC's emphasis on connecting IT risk information to enterprise objectives, governance, and informed response decisions. ISACA describes CRISC as focused on identifying and managing enterprise IT risk and implementing information systems controls; see the official ISACA CRISC certification page. ISACA's broader risk guidance also emphasizes communication and business alignment in technology risk management, as reflected in resources available through ISACA IT Risk resources.

QUESTION NO: 136

Which of the following is the ULTIMATE objective of implementing technical controls in the IT environment?

A. Enhancing the maturity of the IT control environment

B. Reducing regulatory risk

C. Minimizing the likelihood of a threat exposure

D. Optimizing the cost of IT resources

ANSWER: C

Explanation:

Minimizing the likelihood of a threat exposure is correct because technical controls are implemented to reduce the probability that threats can successfully exploit vulnerabilities in IT systems. In risk management terms, controls are safeguards or countermeasures that modify risk, typically by reducing likelihood, reducing impact, or improving detection and response. Technical controls such as access restrictions, encryption, secure configuration, network segmentation, vulnerability management, and monitoring are designed to prevent or limit exposure to unauthorized access, misuse, disruption, or compromise. From a CRISC perspective, the value of a control is ultimately tied to how it contributes to risk reduction in alignment with business objectives and the organization's risk appetite. This aligns with COBIT's governance view that information and technology controls should support enterprise objectives by managing risk appropriately; see ISACA COBIT resources. NIST also defines security controls as safeguards or countermeasures prescribed to protect information systems and reduce risk, reinforcing the same principle; see the NIST definition of security control.

QUESTION NO: 137

Of the following, whose input is ESSENTIAL when developing risk scenarios for the implementation of a third-party mobile application that stores customer data?

A. Information security manager

B. IT vendor manager

C. Business process owner

D. IT compliance manager

ANSWER: C

Explanation:

Business process owner is correct because risk scenarios must be grounded in the business context: how the mobile application supports the organization, what customer data is involved, what processes depend on it, and what business impact could result if confidentiality, integrity, availability, compliance, or customer trust are affected. In ISACA-aligned risk management, technology risk is evaluated in terms of business objectives and enterprise impact, not only technical exposure. The business process owner is the party best positioned to define process criticality, data usage, acceptable levels of disruption, customer-facing consequences, and the value at risk. That input is essential for making the scenario realistic and for ensuring the resulting assessment supports appropriate risk response decisions. Other stakeholders may provide important supporting details, but the business process owner provides the authoritative business perspective needed to frame and prioritize the scenario. This aligns with ISACA's emphasis on governance, risk ownership, and business-focused control objectives as reflected in COBIT resources and ISACA's terminology around risk and accountability in the ISACA glossary.

QUESTION NO: 138

When is the BEST to identify risk associated with major project to determine a mitigation plan?

A. Project execution phase

B. Project initiation phase

C. Project closing phase

D. Project planning phase

ANSWER: D

Explanation:

Project planning phase is correct because this is when the project team has enough detail about objectives, scope, deliverables, dependencies, resources, timelines and constraints to identify meaningful risks and define practical mitigation plans before major work begins. In CRISC and broader IT risk practice, risk management should be proactive and integrated into decision-making, not treated as an after-the-fact activity. During planning, identified risks can still influence the project approach, budget, schedule, control design, acceptance criteria and escalation paths. This timing also enables risk responses to be approved, assigned to accountable owners and embedded into the project plan before execution creates cost, schedule or control impacts. Project risk management guidance similarly treats risk identification and response planning as core planning activities, because mitigation is most effective when it is designed before risk events occur. See ISACA's CRISC overview for the emphasis on identifying and managing enterprise IT risk, and PMI's project risk management resources for project risk practices: ISACA CRISC and PMI Practice Standard for Project Risk Management.

QUESTION NO: 139

Which of the following BEST enables the identification of trends in risk levels?

A. Correlation between risk levels and key risk indicators (KRIs) is positive.

B. Measurements for key risk indicators (KRIs) are repeatable

C. Quantitative measurements are used for key risk indicators (KRIs).

D. Qualitative definitions for key risk indicators (KRIs) are used.

ANSWER: B

Explanation:

Measurements for key risk indicators (KRIs) are repeatable is correct because trend identification depends on comparing like-for-like measurements across multiple reporting periods. A KRI is useful for monitoring risk exposure only when the metric is collected consistently, using the same definition, scope, method, frequency and thresholds over time. Repeatability gives risk managers confidence that changes in reported values reflect actual movement in the underlying risk condition, rather than variation caused by inconsistent measurement practices. In CRISC terms, KRIs support risk monitoring by providing ongoing signals about whether risk exposure is increasing, decreasing or remaining stable; that monitoring is meaningful only when the measurement process can be reproduced reliably. This aligns with common guidance on metrics programs, where consistent and repeatable measures are essential for baselining, comparison and trend analysis. ISACA discusses the role of KRIs in supporting operational risk monitoring and decision making in its Journal guidance on key risk indicators. NIST also emphasizes repeatable information security measurement practices for analyzing performance and change over time in SP 800-55 Rev. 1.

QUESTION NO: 140

Mortality tables are based on what mathematical activity?

Each correct answer represents a complete solution. (Choose three.)

A. Normal distributions

B. Probabilities

C. Impact

D. Sampling

ANSWER: A B D

Explanation:

Mortality tables are built using statistical and actuarial methods that estimate the likelihood of death across defined age groups or populations. Probabilities is correct because a mortality table expresses the chance that a person in a given cohort will die within a specified period, which is fundamentally a probability calculation. Sampling is also correct because mortality assumptions are derived from observed data collected from populations or representative groups; actuaries use those observations to infer patterns for a broader population. Normal distributions is correct in the broader statistical sense because mortality analysis relies on distribution-based modeling to understand how observed outcomes vary around expected values and to support prediction across large datasets. In risk management terms, these methods help convert historical observations into defensible estimates of frequency and likelihood, which is directly relevant when quantifying risk exposure. Authoritative actuarial sources describe mortality tables as statistical tools based on observed death rates and probabilities; for example, see the Society of Actuaries overview of mortality and improvement research and the U.S. Social Security Administration's period life table, which presents age-based probabilities of death.

QUESTION NO: 141

Which of the following potential scenarios associated with the implementation of a new database technology presents the GREATEST risk to an organization?

A. The organization may not have a sufficient number of skilled resources.

B. Application and data migration cost for backups may exceed budget.

C. Data may not be recoverable due to system failures.

D. The database system may not be scalable in the future.

ANSWER: C

Explanation:

Data may not be recoverable due to system failures is the correct answer because loss of recoverability directly threatens the organization's ability to restore critical information assets and resume business operations after an outage, corruption event, or technology failure. In risk terms, this scenario combines potentially severe business impact with uncertainty introduced by implementing a new database platform. If data cannot be recovered, the consequences may include prolonged service disruption, regulatory exposure, loss of customer trust, financial loss, and impaired decision-making. ISACA risk management guidance emphasizes evaluating risk based on business impact and the organization's ability to protect and recover information assets, making recoverability a core concern for technology changes. Similarly, business continuity and disaster recovery practices require that systems supporting important business processes have defined recovery capabilities, validated backups, and tested restoration procedures. Authoritative guidance such as NIST contingency planning highlights backup and recovery as essential controls for maintaining operational resilience, and ISACA describes information and technology risk in terms of events that can affect enterprise objectives. See NIST SP 800-34 Contingency Planning Guide and ISACA IT Risk resources.

QUESTION NO: 142

You are the project manager for your organization. You are preparing for the quantitative risk analysis. Mark, a project team member, wants to know why you need to do quantitative risk analysis when you just completed qualitative risk analysis. Which one of the following statements best defines what quantitative risk analysis is?

A. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.

B. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.

C. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.

D. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.

ANSWER: C

Explanation:

Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives is correct because it captures the key distinction between qualitative and quantitative risk work. After risks have been identified and typically prioritized through qualitative assessment, quantitative analysis uses numerical methods to estimate their potential effect on objectives such as cost, schedule, scope, and performance. This may involve techniques such as expected monetary value, sensitivity analysis, decision trees, or simulation to model uncertainty and understand the range of possible outcomes. The value of this step is that it gives decision makers measurable information about risk exposure, helping them determine contingency reserves, compare response strategies, and understand the likelihood of meeting project targets. This aligns with widely accepted project risk management guidance, including the PMI PMBOK Guide, which treats quantitative risk analysis as a numerical evaluation of uncertainty's impact on project objectives. It is also consistent with risk management principles emphasized in ISACA CRISC, where risk analysis supports informed decisions about treatment and control priorities.

QUESTION NO: 143

Which of the following is the BEST indication that an organization is following a mature risk management process?

A. Executive management receives periodic risk awareness training.

B. Attributes of each risk scenario have been documented within the risk register.

C. The risk register is frequently utilized for decision-making.

D. A dashboard has been developed for senior management to provide real-time risk values.

ANSWER: C

Explanation:

The risk register is frequently utilized for decision-making is the best indication of a mature risk management process because maturity is demonstrated when risk information is embedded into how the organization prioritizes initiatives, allocates resources, selects responses, and makes business decisions. A risk register is not merely a documentation repository; in a mature environment it becomes an active management tool that supports risk-informed decisions and aligns risk treatment with business objectives and risk appetite. This reflects the core CRISC emphasis that risk management should create business value by helping stakeholders understand exposure and choose appropriate responses, rather than simply producing reports or maintaining artifacts. ISACA's risk guidance consistently links effective risk management with business decision support and governance, as reflected in its COBIT materials on aligning governance objectives with enterprise goals: ISACA COBIT Resources. Similarly, NIST describes risk management as a process that informs organizational decisions about mission, business functions, and information systems: NIST Risk Management Framework. Frequent use of the risk register in decision-making shows that risk practices are integrated, repeatable, and valuable to management.

QUESTION NO: 144

You are the project manager of the AFD project for your company. You are working with the project team to reassess existing risk events and to identify risk events that have not happened and whose relevancy to the project has passed. What should you do with these events that have not happened and would not happen now in the project?

A. Add the risk to the issues log

B. Close the outdated risks

C. Add the risks to the risk register

D. Add the risks to a low-priority watch-list

ANSWER: B

Explanation:

Close the outdated risks is correct because risk management is an ongoing activity, not a one-time identification exercise. During periodic risk reassessment, the project manager and team review previously identified risk events to determine whether they are still applicable, whether their probability or impact has changed, and whether any response plans remain necessary. If a risk event has not occurred and the conditions that could trigger it no longer exist, the risk is no longer relevant to the project and should be formally closed or retired. This keeps the risk register focused on current, actionable risks and avoids wasting management attention on events that can no longer affect objectives. In good governance practice, the closure should still be documented so there is an audit trail showing why the risk was retired and when the decision was made. This aligns with ISACA's emphasis on continuous risk identification, analysis, response, and monitoring, as reflected in the CRISC certification domain focus, and with common project risk management practice described by PMI in its risk analysis guidance.

QUESTION NO: 145

When evaluating enterprise IT risk management it is MOST important to:

A. create new control processes to reduce identified IT risk scenarios

B. confirm the organization's risk appetite and tolerance

C. report identified IT risk scenarios to senior management

D. review alignment with the organization's investment plan

ANSWER: B

Explanation:

Confirm the organization's risk appetite and tolerance is correct because enterprise IT risk management can only be evaluated meaningfully against the level of risk the enterprise is willing to accept in pursuit of its objectives. Risk appetite provides the broad boundary for acceptable risk exposure, while risk tolerance translates that appetite into more specific limits that guide decision making, prioritization, and escalation. In a CRISC context, evaluating IT risk management is not just about identifying risks or implementing controls; it is about determining whether risk-related practices, residual risk levels, and treatment decisions are aligned with business objectives and approved governance direction. Without first confirming risk appetite and tolerance, there is no authoritative benchmark for judging whether identified IT risks are acceptable, require mitigation, should be transferred, or need executive attention. This aligns with ISACA's emphasis on risk governance and business alignment in IT risk management. See ISACA's IT risk resources at ISACA IT Risk and ISACA's definitions and governance terminology in the ISACA Glossary.

QUESTION NO: 146

You are the project manager of a project in Bluewell Inc. You and your project team have identified several project risks, completed risk analysis, and are planning to apply most appropriate risk responses. Which of the following tools would you use to choose the appropriate risk response?

A. Project network diagrams

B. Cause-and-effect analysis

C. Decision tree analysis

D. Delphi Technique

ANSWER: C

Explanation:

Decision tree analysis is correct because it is specifically used to evaluate alternative courses of action under uncertainty and select the response that provides the most favorable expected outcome. After risks have been identified and analyzed, the project manager needs a structured way to compare possible responses by considering probability, impact, cost, and expected value. A decision tree visually maps decision points, uncertain events, possible outcomes, and associated payoffs or losses, allowing the team to compare response strategies using expected monetary value or similar quantitative criteria. This aligns well with risk response planning because the goal is not merely to understand a risk, but to choose the action that best optimizes value while staying within the organization's risk appetite and project constraints. ISACA's risk guidance emphasizes informed risk decisions and response selection based on business impact and risk tolerance, and decision tree analysis supports that by making assumptions, alternatives, and consequences explicit. For more context, see ISACA's risk terminology resources at ISACA Glossary and PMI's discussion of decision tree analysis and expected monetary value at PMI.

QUESTION NO: 147

What are the functions of audit and accountability control?

Each correct answer represents a complete solution. (Choose three.)

A. Provides details on how to protect the audit logs

B. Implement effective access control

C. Implement an effective audit program

D. Provides details on how to determine what to audit

ANSWER: A C D

Explanation:

Audit and accountability controls are intended to establish a reliable audit capability that supports monitoring, investigation, reporting, and accountability for system activity. "Implement an effective audit program" is correct because this control area defines the practices needed to generate, review, analyze, retain, and use audit records as part of governance and security oversight. "Provides details on how to determine what to audit" is also correct because audit planning must identify auditable events, required content of audit records, and the events that are significant enough to support security objectives and investigations. "Provides details on how to protect the audit logs" is correct because audit records must be protected from unauthorized access, modification, deletion, and loss so they remain trustworthy and usable for accountability and potential non-repudiation. These concepts align with the NIST SP 800-53 Audit and Accountability control family, which covers audit event selection, audit record content, audit review and analysis, audit record protection, and audit record retention. See the NIST SP 800-53 Rev. 5 publication and the NIST AU-2 Event Logging control.

QUESTION NO: 148

Which of the following steps ensure effective communication of the risk analysis results to relevant stakeholders? Each correct answer represents a complete solution. (Choose three.)

A. The results should be reported in terms and formats that are useful to support business decisions

B. Provide decision makers with an understanding of worst-case and most probable scenarios,due diligence exposures and significant reputation, legal or regulatory considerations

C. Communicate the negative impacts of the events only, it needs more consideration

D. Communicate the risk-return context clearly

ANSWER: A B D

Explanation:

Effective communication of risk analysis results means presenting risk information in a way that supports informed business decision making. “The results should be reported in terms and formats that are useful to support business decisions” is correct because risk analysis is valuable only when stakeholders can understand, compare and act on the information. “Provide decision makers with an understanding of worst-case and most probable scenarios,due diligence exposures and significant reputation, legal or regulatory considerations” is also correct because senior management and risk owners need scenario-based context to evaluate exposure, obligations and business impact. “Communicate the risk-return context clearly

” is correct because CRISC-aligned risk communication should help stakeholders balance exposure against value, including likelihood, impact, uncertainty and the potential return from accepting or treating risk. This aligns with ISACA’s CRISC focus on IT risk identification, assessment, response and reporting, and with widely accepted risk assessment guidance that risk results should be communicated to organizational decision makers in a usable form. See ISACA’s CRISC overview at ISACA CRISC and NIST guidance on communicating risk assessment results at NIST SP 800-30 Rev. 1.

QUESTION NO: 149

The PRIMARY purpose of IT control status reporting is to:

A. ensure compliance with IT governance strategy.

B. assist internal audit in evaluating and initiating remediation efforts.

C. benchmark IT controls with Industry standards.

D. facilitate the comparison of the current and desired states.

ANSWER: D

Explanation:

The correct answer is **facilitate the comparison of the current and desired states.** IT control status reporting is primarily a monitoring and communication activity: it gives management and other stakeholders a clear view of how existing controls are performing against defined objectives, risk appetite, control requirements and target maturity or capability levels. In an ISACA-aligned risk and control environment, reporting should support oversight and decision-making by showing whether controls are operating as intended, where gaps exist and whether remediation is moving the organization toward the target state. This is consistent with COBIT’s emphasis on monitoring performance, conformance and achievement of enterprise and alignment goals through meaningful information for governance and management. In CRISC terms, effective control reporting helps risk owners understand residual risk and control effectiveness so they can prioritize action and track improvement over time. The key point is that reporting itself does not “ensure” compliance or perform remediation; its primary value is making the difference between the current control posture and the desired control posture visible and actionable. See ISACA’s COBIT resources at ISACA COBIT and CRISC certification domain context at ISACA CRISC.

QUESTION NO: 150

What are the PRIMARY requirements for developing risk scenarios?

Each correct answer represents a part of the solution. (Choose two.)

A. Potential threats and vulnerabilities that could lead to loss events

B. Determination of the value of an asset at risk

C. Determination of actors that has potential to generate risk

D. Determination of threat type

ANSWER: A B

Explanation:

Potential threats and vulnerabilities that could lead to loss events and Determination of the value of an asset at risk are the primary requirements for developing meaningful risk scenarios. In ISACA-aligned risk practice, a risk scenario should describe how a loss event could occur and what business value could be affected. This means the scenario must connect a valuable asset, information resource, or business process with plausible sources of harm, such as threats exploiting vulnerabilities, so the organization can estimate business impact and likelihood in a useful way. Without knowing what is at risk, the scenario cannot be tied to business objectives or evaluated for significance. Without identifying the threats and vulnerabilities that could create a loss event, the scenario lacks the causal basis needed for assessment, prioritization, and response planning. This approach is consistent with ISACA's risk scenario thinking, where scenarios support business-focused IT risk analysis, and with widely used risk assessment guidance such as NIST SP 800-30, which links threats, vulnerabilities, likelihood, and impact in risk determination. See ISACA IT Risk resources and NIST SP 800-30 Revision 1.

QUESTION NO: 151

Which of the following would MOST likely result in updates to an IT risk appetite statement?

A. Changes in senior management

B. External audit findings

C. Feedback from focus groups

D. Self-assessment reports

ANSWER: A

Explanation:

Changes in senior management is correct because an IT risk appetite statement expresses the amount and type of IT-related risk the organization is willing to accept in pursuit of its objectives. That appetite is not just an operational metric; it is a governance-level position that should reflect the organization's strategy, priorities, risk culture, and leadership expectations. When senior management changes, the organization may adopt different business objectives, investment priorities, digital transformation goals, compliance expectations, or tolerance for uncertainty. Since IT risk appetite must remain aligned with enterprise direction and executive decision-making, such a leadership change is highly likely to trigger a review and possible update of the statement.

ISACA's IT risk guidance emphasizes that risk appetite and tolerance are set through governance and should align with enterprise objectives and stakeholder expectations. Similarly, enterprise risk management guidance treats risk appetite as a board and executive-level expression that supports strategy and performance decisions. See ISACA's overview of IT risk management at ISACA IT Risk and COSO's ERM guidance at COSO Enterprise Risk Management.

QUESTION NO: 152

You are the project manager of the NKJ Project for your company. The project's success or failure will have a significant impact on your organization's profitability for the coming year. Management has asked you to identify the risk events and communicate the event's probability and impact as early as possible in the project. Management wants to avoid risk events and needs to analyze the cost-benefits of each risk event in this project. What term is assigned to the low-level of stakeholder tolerance in this project?

A. Mitigation-ready project management

B. Risk avoidance

C. Risk utility function

D. Risk-reward mentality

ANSWER: C

Explanation:

Risk utility function is correct because it represents how much value, satisfaction, or “utility” stakeholders associate with accepting a given level of risk. In risk management, stakeholder tolerance is not just a qualitative preference; it can be modeled as a utility relationship that shows whether decision makers are risk seeking, risk neutral, or risk averse. A low level of stakeholder tolerance indicates that management gains little perceived value from taking risk and strongly prefers reducing uncertainty, which is exactly the kind of attitude a risk utility function is used to express.

For a project with major profitability implications, early communication of probability, impact, and cost-benefit information supports decisions that align with the organization’s appetite and tolerance for risk. This is consistent with CRISC’s focus on identifying, analyzing, evaluating, and responding to IT and enterprise risk in a way that supports business objectives, as outlined by ISACA CRISC. The idea also aligns with the general definition of risk tolerance as the acceptable level of variation relative to objectives, reflected in resources such as the NIST risk tolerance glossary.

QUESTION NO: 153

Which of the following is MOST important when identifying an organization's risk exposure associated with Internet of Things (IoT) devices?

A. Defined remediation plans

B. Management sign-off on the scope

C. Manual testing of device vulnerabilities

D. Visibility into all networked devices

ANSWER: D

Explanation:

Visibility into all networked devices is the most important factor because risk exposure cannot be reliably identified without first knowing what IoT assets exist, where they are connected, how they communicate, and what business processes they support. IoT environments often include unmanaged, embedded, or intermittently connected devices that may not be covered by traditional endpoint inventories. From a risk management perspective, complete asset discovery and inventory provide the foundation for determining threat exposure, vulnerability presence, control gaps, data flows, and potential business impact. This aligns with recognized cybersecurity practices that treat asset identification as a prerequisite for effective risk assessment and control selection. NIST guidance for IoT device cybersecurity emphasizes understanding device capabilities, interfaces, and network interactions as part of managing IoT cybersecurity risk; see NIST SP 800-213. Similarly, NISTIR 8259 highlights IoT device identification and cybersecurity capabilities as important inputs to managing IoT-related risk; see NISTIR 8259. Without this visibility, the organization’s exposure assessment is incomplete and may overlook significant unmanaged risk.

QUESTION NO: 154

What are the various outputs of risk response?

A. Risk Priority Number

B. Residual risk

C. Risk register updates

D. Project management plan and Project document updates

E. Risk-related contract decisions

ANSWER: C D E

Explanation:

The correct outputs of risk response are Risk register updates, Project management plan and Project document updates, and Risk-related contract decisions. In risk response planning, the selected response actions must be documented so they

can be assigned, tracked, funded, scheduled, and monitored. Risk register updates capture the agreed response strategy, risk owners, contingency plans, triggers, and any changes to probability, impact, or priority after response planning. Project management plan and Project document updates are also outputs because approved responses can affect baselines, schedules, budgets, resources, procurement plans, assumptions, and technical documentation. Risk-related contract decisions are valid outputs when a response involves transferring or sharing risk through insurance, outsourcing, warranties, service agreements, or other contractual mechanisms. These outputs align with widely accepted project risk management practice, where planning risk responses produces changes to project documents and plans and may drive procurement or contractual action. ISACA's risk guidance similarly emphasizes selecting and documenting response actions so risk can be treated, owned, and monitored within governance processes; see ISACA Journal: Risk Response Considerations. For the project management framing of risk response outputs and documentation, see PMI risk management strategies, tools and techniques.

QUESTION NO: 155

Which of the following is the MOST critical security consideration when an enterprise outsource is major part of IT department to a third party whose servers are in foreign company?

A. A security breach notification may get delayed due to time difference

B. The enterprise could not be able to monitor the compliance with its internal security and privacy guidelines

C. Laws and regulations of the country of origin may not be enforceable in foreign country

D. Additional network intrusion detection sensors should be installed, resulting in additional cost

ANSWER: C

Explanation:

Laws and regulations of the country of origin may not be enforceable in foreign country is the correct answer because outsourcing IT operations to a provider operating servers in another jurisdiction creates a legal, regulatory and data sovereignty risk that can materially affect the enterprise's ability to protect information and meet compliance obligations. In CRISC terms, this is a critical risk scenario because accountability for risk remains with the enterprise even when service delivery is transferred to a third party. If data is stored, processed or accessed in a foreign country, local privacy laws, government access rules, breach obligations, contractual enforceability, evidence discovery rules and regulatory expectations may differ from those in the enterprise's home country. That can limit the enterprise's ability to enforce controls, obtain timely remedies, demonstrate compliance, or ensure that security and privacy requirements are legally binding. Strong third-party risk management therefore requires evaluating jurisdiction, applicable laws, contractual protections, audit rights and data handling requirements before outsourcing. This aligns with ISACA's emphasis on governance and vendor risk management, as well as NIST guidance that outsourced IT security responsibilities must be clearly addressed contractually and legally. See ISACA Journal: Vendor Management Using COBIT 5 and NIST SP 800-35, Guide to Information Technology Security Services.

QUESTION NO: 156

An IT license audit has revealed that there are several unlicensed copies of commercial applications installed on company laptops. The risk practitioner's BEST course of action would be to:

A. immediately uninstall the unlicensed software from the laptops.

B. procure the requisite licenses for the software to minimize business impact.

C. report the issue to management so appropriate action can be taken.

D. centralize administration rights on laptops so that installations are controlled.

ANSWER: C

Explanation:

“report the issue to management so appropriate action can be taken” is correct because the risk practitioner’s role is to identify, assess, communicate, and monitor risk—not to unilaterally choose or execute the business response. Unlicensed commercial software creates legal, compliance, financial, and reputational exposure, and it may also indicate a weakness in software asset management controls. The appropriate first step is to escalate the audit finding to the accountable management or risk owner so the issue can be evaluated in context and a formal risk response can be selected, approved, funded, and tracked. This aligns with CRISC’s focus on risk governance and risk response, where management owns risk decisions and the risk practitioner supports those decisions with accurate risk information and monitoring. Reporting the issue enables management to determine the appropriate remediation path, such as licensing, removal, disciplinary action, control improvements, or a combination of actions, while ensuring accountability and documentation. ISACA describes CRISC as validating expertise in identifying and managing enterprise IT risk and implementing information systems controls; see ISACA CRISC. Related governance principles are also reflected in ISACA’s COBIT resources, which emphasize management objectives, accountability, and controlled responses to enterprise IT issues: ISACA COBIT.

QUESTION NO: 157

You are the project manager of GHT project. You have analyzed the risk and applied appropriate controls. In turn, you got residual risk as a result of this. Residual risk can be used to determine which of the following?

A. Status of enterprise's risk

B. Appropriate controls to be applied next

C. The area that requires more control

D. Whether the benefits of such controls outweigh the costs

ANSWER: C D

Explanation:

Residual risk is the level of risk that remains after risk responses and controls have been applied. In ISACA-aligned risk management practice, management evaluates residual risk to decide whether the remaining exposure is acceptable, whether additional treatment is needed, and whether the cost of further control is justified by the reduction in risk. Therefore, **The area that requires more control** is correct because residual risk highlights where exposure remains above the organization’s risk appetite or tolerance, indicating where stronger, additional, or improved controls may be needed.

Whether the benefits of such controls outweigh the costs is also correct because residual risk supports cost-benefit decision-making. If the remaining risk is still material, management can compare the expected reduction in exposure against the cost, effort, and business impact of implementing additional controls. This aligns with the CRISC focus on risk response, mitigation, and control optimization, where controls should be proportionate to business risk and value. ISACA’s CRISC exam content emphasizes analyzing risk scenarios and determining appropriate risk responses and controls; see the ISACA CRISC Exam Content Outline. NIST also defines residual risk as the risk remaining after controls are implemented, reinforcing its role in deciding whether further treatment is necessary; see the NIST residual risk glossary.

QUESTION NO: 158

Which of the following comes under phases of risk management?

A. Assessing risk

B. Prioritization of risk

C. Identify risk

D. Monitoring risk

E. Developing risk

ANSWER: A B C D

Explanation:

Assessing risk, Prioritization of risk, Identify risk, and Monitoring risk are all recognized phases or activities within a sound risk management lifecycle. In CRISC-aligned practice, risk management begins with identifying risk events, assets, threats, vulnerabilities, and business conditions that may affect enterprise objectives. Once risks are identified, assessing risk is needed to estimate likelihood, impact, and overall exposure, often using qualitative and quantitative methods. Prioritization of risk then helps the enterprise focus resources on the risks that matter most, based on severity, business impact, risk appetite, and urgency. Monitoring risk is also essential because risk is not static; control effectiveness, threat conditions, business processes, and technology environments change over time, requiring ongoing review and reporting. This structure is consistent with ISACA's CRISC focus on IT risk identification, assessment, response, and monitoring/reporting, as reflected in the ISACA CRISC certification overview. It also aligns with broader risk management good practice described in the NIST Risk Management Framework, where risks are selected, assessed, responded to, and continuously monitored as part of a lifecycle approach.

QUESTION NO: 159

Qualitative risk assessment uses which of the following terms for evaluating risk level?

Each correct answer represents a part of the solution. (Choose two.)

A. Impact

B. Annual rate of occurrence

C. Probability

D. Single loss expectancy

ANSWER: A C

Explanation:

Qualitative risk assessment evaluates risk by estimating the likelihood that a risk event will occur and the severity of the consequences if it does occur. In common risk-management practice, those two factors are expressed as Probability and Impact. Probability represents the chance or likelihood of occurrence, often using descriptive scales such as low, medium and high. Impact represents the expected business or operational effect, also commonly expressed using qualitative ratings rather than precise monetary values. Together, Probability and Impact are used to determine or prioritize the overall risk level, frequently through a risk matrix or similar scoring model.

This approach is consistent with ISACA-aligned risk management concepts, where risk analysis considers likelihood and impact to support prioritization and response decisions. It is also consistent with widely used risk assessment guidance such as NIST SP 800-30, which describes risk as a function of likelihood and impact. See ISACA's discussion of risk assessment practices at ISACA Journal: Performing a Risk Assessment and NIST's risk assessment guidance at NIST SP 800-30 Rev. 1.

QUESTION NO: 160

Which of the following is MOST important for the organization to consider before implementing a new in-house developed artificial intelligence (AI) solution?

A. Industry trends in AI

B. Expected algorithm outputs

C. Data feeds

D. Alert functionality

ANSWER: B

Explanation:

Expected algorithm outputs is correct because an organization should first understand and define what the artificial intelligence solution is expected to produce before it is placed into operation. For an in-house AI implementation, expected outputs provide the basis for validating whether the model supports the business objective, whether its results are explainable enough for intended use, and whether performance, accuracy, bias, and control thresholds can be evaluated. In CRISC terms, this is a risk-and-control concern: without a defined target outcome, the organization cannot reliably assess whether the AI solution introduces unacceptable operational, compliance, ethical, or decision-quality risk. Establishing expected outputs also supports acceptance testing, monitoring, accountability, and ongoing governance after deployment. This aligns with AI risk management guidance emphasizing that AI systems should be mapped to intended purpose, context, performance expectations, and impacts before implementation. See the NIST AI Risk Management Framework for guidance on mapping and measuring AI system risks, and ISACA's AI governance resources such as the ISACA AI Audit Toolkit announcement, which highlights the need to evaluate AI governance, risk, and control considerations.

QUESTION NO: 161

You work as the project manager for Bluewell Inc. There has been a delay in your project work that is adversely affecting the project schedule. You decide, with your stakeholders' approval, to fast track the project work to get the project done faster. When you fast track the project, what is likely to increase?

A. Human resource needs

B. Quality control concerns

C. Costs

D. Risks

ANSWER: D

Explanation:

Risks is correct because fast tracking compresses the project schedule by performing activities or phases in parallel that would normally be performed sequentially. This can help recover lost time, but it reduces the natural dependencies, review points, and learning opportunities that exist in a sequential plan. As a result, teams may have to make decisions with less complete information, rework may become more likely, coordination complexity increases, and unresolved issues from one activity can affect another activity that has already started. In project risk terms, fast tracking changes the execution approach in a way that can increase uncertainty and the probability or impact of adverse events. This aligns with standard project management guidance, where fast tracking is treated as a schedule compression technique that commonly increases risk exposure. It also fits the CRISC perspective that changes to plans, processes, or controls should be evaluated for their effect on risk. See the PMI PMBOK® Guide standards page and ISACA's overview of IT risk for related risk management context.

QUESTION NO: 162

A cloud service provider has completed upgrades to its cloud infrastructure to enhance service availability. Which of the following is the MOST important key risk indicator (KRI) for management to monitor?

A. Percentage of technology upgrades resulting in security breaches

B. Percentage of servers not patched per policy

C. Number of incidents with downtime exceeding contract threshold

D. Peak demand on the cloud service during business hours

ANSWER: C

Explanation:

Number of incidents with downtime exceeding contract threshold is the most important KRI because it directly measures whether the upgraded cloud infrastructure is failing to meet the availability level that matters most to the provider and its

customers: the contractual service commitment. In a CRISC context, a key risk indicator should provide management with meaningful insight into exposure against risk appetite, tolerance, or agreed service expectations. For a cloud service provider, downtime beyond the agreed threshold represents a concrete risk event tied to service availability, customer impact, potential penalties, reputational damage, and management accountability. Monitoring this KRI enables management to determine whether the infrastructure upgrades are actually reducing availability risk and whether further corrective action, capacity planning, resilience improvements, or incident response changes are needed. ISACA describes KRIs as indicators used to monitor risk exposure and support risk-informed decision-making; see the ISACA Glossary. Cloud availability and service levels are also commonly governed through measurable service-level commitments, as reflected in cloud computing guidance from NIST SP 800-145.

QUESTION NO: 163

Which of the following are sub-categories of threat?

Each correct answer represents a complete solution. (Choose three.)

A. Natural and supernatural

B. Computer and user

C. Natural and man-made

D. Intentional and accidental

E. External and internal

ANSWER: C D E

Explanation:

Natural and man-made, Intentional and accidental, and External and internal are correct because they reflect common ways to classify threat sources and threat events in information risk management. Natural and man-made distinguishes events arising from environmental or physical causes, such as earthquakes, storms, floods, and fires, from events caused by people or organizations. Intentional and accidental separates deliberate harmful activity, such as fraud, sabotage, misuse, or cyberattack, from unintentional events such as human error, misconfiguration, or accidental data disclosure. External and internal identifies whether the threat originates outside the organization's control boundary, such as criminals, competitors, suppliers, or environmental events, or from within the organization, such as employees, contractors, processes, or internally managed technology. These categories help risk practitioners build a more complete threat inventory, understand likely threat sources, and select suitable controls based on origin, intent, and nature of the threat. This approach aligns with recognized risk assessment practices, including NIST's discussion of adversarial, non-adversarial, human, and environmental threat sources in NIST SP 800-30 Revision 1, and with ISACA's risk-management terminology and guidance available through the ISACA Glossary.

QUESTION NO: 164

Who should be accountable for authorizing information system access to internal users?

A. Information custodian

B. Information owner

C. Information security officer

D. Information security manager

ANSWER: B

Explanation:

Information owner is correct because access authorization is a business accountability tied to the value, sensitivity, and permitted use of the information. In ISACA-aligned governance and risk management practices, the owner of the information

is the role that understands the business purpose of the data, the impact of inappropriate disclosure or modification, and the legitimate need-to-know requirements for users. Therefore, the information owner is accountable for deciding who should have access and at what level, ensuring those decisions align with business requirements, risk appetite, classification, and regulatory obligations. This accountability also supports separation of duties: access can be technically provisioned by operational teams, but the authority to approve access should remain with the business role responsible for the information asset. NIST uses a similar concept, describing an information owner as an official with authority for specified information and responsibility for establishing controls for its generation, collection, processing, dissemination, and disposal. See the NIST CSRC definition of information owner and NIST guidance on access control in SP 800-53.

QUESTION NO: 165

Which of the following is the MAIN reason to continuously monitor IT-related risk?

A. To ensure risk levels are within acceptable limits of the organization's risk appetite and risk tolerance

B. To redefine the risk appetite and risk tolerance levels based on changes in risk factors

C. To help identify root causes of incidents and recommend suitable long-term solutions

D. To update the risk register to reflect changes in levels of identified and new IT-related risk

ANSWER: A

Explanation:

To ensure risk levels are within acceptable limits of the organization's risk appetite and risk tolerance is correct because continuous IT risk monitoring is fundamentally about maintaining an up-to-date view of whether current exposure remains acceptable to the enterprise. In CRISC-oriented risk management, risk appetite defines the broad level of risk the organization is willing to pursue or retain, while risk tolerance translates that appetite into more specific acceptable variation or thresholds. Monitoring provides the evidence needed to detect when changing threats, vulnerabilities, control performance, business conditions, or technology dependencies cause actual risk to move outside those approved boundaries. This enables timely escalation and risk response decisions aligned with governance expectations and business objectives. ISACA's risk guidance emphasizes that risk management should support enterprise objectives and decision-making, which depends on understanding whether risk remains within agreed limits; see ISACA Journal: Using Risk Management to Align IT With Business Strategy. Similarly, NIST describes monitoring as an ongoing activity to determine whether risk responses remain effective and risk remains acceptable; see NIST SP 800-37 Rev. 2.

QUESTION NO: 166

Which of the following guidelines should be followed for effective risk management?

Each correct answer represents a complete solution. (Choose three.)

A. Promote and support consistent performance in risk management

B. Promote fair and open communication

C. Focus on enterprise's objective

D. Balance the costs and benefits of managing risk

ANSWER: B C D

Explanation:

Effective risk management should be business-driven, transparent, and economically justified. "Promote fair and open communication" is correct because risk decisions depend on timely, accurate, and transparent information being shared among stakeholders. Without open communication, decision makers cannot understand the likelihood, impact, ownership, or treatment status of risk. "Focus on enterprise's objective" is correct because ISACA's risk management guidance emphasizes that IT and information-related risk must be understood in the context of enterprise goals and value delivery; risk

is meaningful only when tied to objectives that may be affected. “Balance the costs and benefits of managing risk” is also correct because risk response should be proportionate: controls, mitigation activities, monitoring, and assurance should provide value relative to the risk reduction achieved. This aligns with the risk-based approach reflected in ISACA’s CRISC body of knowledge and broader risk management standards, where risk treatment is selected based on business impact, stakeholder expectations, and value considerations. For reference, see ISACA’s overview of IT risk management at ISACA IT Risk and ISO’s summary of risk management principles at ISO 31000 Risk Management.

QUESTION NO: 167

Which of the following would be the BEST way to help ensure the effectiveness of a data loss prevention (DLP) control that has been implemented to prevent the loss of credit card data?

A. Reviewing logs for unauthorized data transfers

B. Configuring the DLP control to block credit card numbers

C. Testing the transmission of credit card numbers

D. Testing the DLP rule change control process

ANSWER: C

Explanation:

Testing the transmission of credit card numbers is correct because control effectiveness is best confirmed by validating that the implemented DLP rule actually detects and prevents the specific data movement it is intended to stop. For a DLP control protecting payment card data, an appropriate effectiveness test would use authorized, controlled test data that matches credit card number patterns and verify that the DLP solution blocks, quarantines, alerts on, or otherwise handles the attempted transmission according to the approved control design. This provides direct evidence that the control is operating as intended in the real environment, rather than merely confirming that a setting exists or that activity is logged after the fact. In risk and control assurance, operating effectiveness is established through testing the control against the risk scenario it is designed to mitigate. PCI DSS also emphasizes protecting account data and validating security controls used to prevent unauthorized disclosure of cardholder data. See the PCI DSS v4.0.1 standard and NIST guidance on assessment and monitoring of security controls in NIST SP 800-53 Revision 5.

QUESTION NO: 168

Which of the following are the principles of risk management?

Each correct answer represents a complete solution. (Choose three.)

A. Risk management should be an integral part of the organization

B. Risk management should be a part of decision-making

C. Risk management is the responsibility of executive management

D. Risk management should be transparent and inclusive

ANSWER: A B D

Explanation:

The correct principles are that risk management should be an integral part of the organization, should be a part of decision-making, and should be transparent and inclusive. These reflect ISO 31000 risk management principles, which emphasize that risk management is not a separate compliance activity but something embedded into governance, strategy, planning, operations, and performance management. When risk management is integrated into the organization, risk information is considered naturally within business processes rather than after decisions have already been made.

Risk management should also be a part of decision-making because its purpose is to help decision makers understand uncertainty, evaluate alternatives, and select actions that support objectives within acceptable risk levels. Transparency and

inclusiveness are also key because effective risk management depends on involving appropriate stakeholders, using relevant knowledge, and ensuring that assumptions, risk criteria, and risk responses are visible enough to support trust and accountability. These principles align with ISO guidance that risk management should be integrated, inclusive, dynamic, and based on the best available information. See ISO 31000 risk management and ISO 31000:2018.

QUESTION NO: 169

An organization has outsourced a critical process involving highly regulated data to a third party with servers located in a foreign country. Who is accountable for the confidentiality of this data?

A. Third-party data custodian

B. Data custodian

C. Regional office executive

D. Data owner

ANSWER: D

Explanation:

Data owner is correct because accountability for protecting information remains with the organization and the individual or role that has authority over the data, even when processing, storage, or administration is outsourced to a third party. In ISACA-aligned governance and risk management practice, the data owner determines classification, acceptable use, protection requirements, and risk decisions for the information. A service provider may operate systems or perform day-to-day handling, but contractual delegation of activities does not transfer ultimate accountability for confidentiality, especially when the data is highly regulated and stored in another jurisdiction. The data owner must ensure that confidentiality requirements are defined, communicated, contractually enforced, monitored, and aligned with applicable legal and regulatory obligations. This includes confirming that cross-border processing risks, privacy requirements, encryption, access controls, audit rights, incident notification, and compliance obligations are appropriately addressed. NIST similarly defines an information owner as the official responsible for establishing rules for appropriate use and protection of information; see the NIST CSRC glossary definition of information owner. ISACA's governance perspective also emphasizes that accountability remains with enterprise roles responsible for information and risk decisions; see the ISACA glossary.

QUESTION NO: 170

Which of the following is the MOST important consideration when sharing risk management updates with executive management?

A. Including trend analysis of risk metrics

B. Using an aggregated view of organizational risk

C. Relying on key risk indicator (KRI) data

D. Ensuring relevance to organizational goals

ANSWER: D

Explanation:

Ensuring relevance to organizational goals is the most important consideration because executive management needs risk information that supports strategic decision-making, prioritization, and accountability. At the executive level, risk updates should not simply report operational details; they should connect risk exposure, control performance, emerging threats, and response status to the organization's objectives, value delivery, and risk appetite. This alignment helps executives understand whether current risk levels could affect business outcomes and whether additional action, funding, or governance direction is needed. ISACA's CRISC exam content emphasizes governance, risk response, and reporting in the context of business objectives and enterprise risk management, which makes strategic relevance central to effective communication with leadership. Similarly, COBIT's governance guidance stresses that information should be relevant, useful, and aligned

with stakeholder needs so that governance bodies can make informed decisions. See ISACA's CRISC exam content outline at ISACA CRISC Exam Content Outline and COBIT information on governance and management of enterprise IT at ISACA COBIT.

QUESTION NO: 171

Which of the following is the MOST important reason to create risk scenarios?

A. To assist with risk identification

B. To determine risk tolerance

C. To determine risk appetite

D. To assist in the development of risk responses

ANSWER: A

Explanation:

To assist with risk identification is correct because risk scenarios are primarily a structured way to describe how an adverse event could occur, what assets or business processes could be affected, and what conditions or threat events could lead to loss. In ISACA risk practices, scenarios make risk concrete and easier for business and IT stakeholders to recognize, discuss, and validate. A well-written scenario links a threat, vulnerability or event, affected asset, business impact, and relevant conditions, which helps uncover risks that might otherwise remain vague or overlooked. Once risks have been identified through scenarios, the organization can then analyze likelihood and impact, compare exposure to risk appetite and tolerance, and decide on appropriate responses. However, those later activities depend on first having a clear, business-relevant expression of the risk event. This is why the most important reason to create risk scenarios is to support risk identification. ISACA's CRISC credential emphasizes IT risk identification as a core practice area, and ISACA risk guidance discusses scenarios as a practical technique for articulating and analyzing risk events. See ISACA CRISC and ISACA Journal: Use of Risk Scenarios in Enterprise Risk Management.

QUESTION NO: 172

You have been assigned as the Project Manager for a new project that involves development of a new interface for your existing time management system. You have completed identifying all possible risks along with the stakeholders and team and have calculated the probability and impact of these risks. Which of the following would you need next to help you prioritize the risks?

A. Affinity Diagram

B. Risk rating rules

C. Project Network Diagram

D. Risk categories

ANSWER: B

Explanation:

Risk rating rules is the correct choice because once probability and impact have been estimated, the next step is to translate those values into a consistent priority or severity level. In practical project and information risk management, this is commonly done through predefined rating criteria, such as a probability-impact matrix, scoring model, or defined thresholds for low, medium, high, and critical risks. These rules ensure that risks are not prioritized subjectively or inconsistently across stakeholders, teams, or projects. They also support defensible decision-making by showing how the calculated likelihood and business impact lead to a specific risk ranking and response priority.

This approach aligns with recognized risk management practice: risk assessment methods evaluate likelihood and impact, then use criteria to determine significance and guide response decisions. ISACA's risk guidance emphasizes structured risk

analysis and evaluation to support prioritization and treatment decisions; see ISACA IT Risk resources. Similarly, NIST SP 800-30 describes risk assessment as using likelihood and impact to determine risk and inform risk response; see NIST SP 800-30 Rev. 1.

QUESTION NO: 173

Which of the following methods is the BEST way to measure the effectiveness of automated information security controls prior to going live?

A. Testing in a non-production environment

B. Performing a security control review

C. Reviewing the security audit report

D. Conducting a risk assessment

ANSWER: A

Explanation:

Testing in a non-production environment is the best way to measure the effectiveness of automated information security controls before go-live because it allows the organization to validate how the controls actually operate under realistic conditions without exposing live systems, business transactions, or sensitive production data to unnecessary risk. Automated controls such as access rules, logging, encryption enforcement, interface validations, and security monitoring must be proven through execution, not only through design review. A properly configured test or staging environment can simulate expected workloads, user activity, integrations, and failure conditions so the organization can confirm that the controls prevent, detect, or respond as intended before implementation. This aligns with the control assessment concept that effectiveness is determined by assessing whether controls are implemented correctly, operating as intended, and producing the desired security outcome, as reflected in NIST guidance on security and privacy control assessments at NIST SP 800-53A. It also supports ISACA's emphasis on validating controls and managing risk before changes affect operations, consistent with governance and control practices described in COBIT resources.

QUESTION NO: 174

An organization must implement changes as the result of new regulations. Which of the following should the risk practitioner do FIRST to prepare for these changes?

A. Engage the legal department.

B. Conduct a gap analysis.

C. Implement compensating controls.

D. Review the risk profile.

ANSWER: B

Explanation:

Conduct a gap analysis. is correct because the risk practitioner must first determine the difference between the organization's current control, process, and compliance posture and the state required by the new regulations. A gap analysis provides the factual basis for planning the change effort: it identifies what requirements are already satisfied, what deficiencies exist, what remediation activities are needed, and where resources should be prioritized. In CRISC-aligned risk management, changes to the regulatory environment should be translated into risk and control implications before action plans are finalized. This supports informed decision-making, avoids unnecessary or misdirected control implementation, and helps management understand the scope, cost, and urgency of the required changes. The approach is consistent with recognized governance and risk practices that emphasize assessing current capability against target requirements before remediation. ISACA's CRISC credential focuses on identifying and managing enterprise IT risk and designing appropriate information systems controls, which aligns with using gap analysis as the initial preparation step: ISACA CRISC. Similarly,

the NIST Cybersecurity Framework describes comparing current and target profiles to identify gaps and actions needed to achieve desired outcomes: NIST Cybersecurity Framework.

QUESTION NO: 175

Which of the following is the PRIMARY benefit of integrating risk and security requirements in an organization ' s enterprise architecture (EA)?

A. Adherence to legal and compliance requirements

B. Reduction in the number of test cases in the acceptance phase

C. Establishment of digital forensic architectures

D. Consistent management of information assets

ANSWER: D

Explanation:

Consistent management of information assets is correct because enterprise architecture provides the organization-wide structure for aligning business processes, information, applications, technology and governance. When risk and security requirements are embedded into that architecture, protection needs are addressed consistently from strategy and design through implementation, operation and retirement. This helps ensure that information assets are identified, classified, protected and monitored in a repeatable way across systems and business units, rather than being handled as isolated project-level concerns. In CRISC terms, this supports effective risk response because controls and security expectations are built into the lifecycle of assets and services, enabling risks to be recognized and treated earlier and more uniformly. ISACA guidance emphasizes that enterprise architecture and cybersecurity should be integrated so security becomes part of business and technology planning rather than an afterthought; see ISACA Journal: Integrating Cybersecurity and Enterprise Architecture. This is also consistent with systems security engineering principles in NIST SP 800-160 Vol. 1 Rev. 1, which promote integrating security and risk considerations throughout system life cycles.

QUESTION NO: 176

What is the MOST important consideration when selecting key performance indicators (KPIs) for control monitoring?

A. Source information is acquired at stable cost

B. Source information is tailored by removing outliers

C. Source information is readily quantifiable

D. Source information is consistently available

ANSWER: D

Explanation:

Source information is consistently available is correct because control monitoring depends on trends, comparisons, thresholds and timely exception reporting. A KPI is useful only when the underlying data can be obtained repeatedly and reliably across monitoring cycles. In a risk and control environment, management needs to know whether a control continues to operate within expected performance boundaries; that requires a stable stream of source information so the KPI can be measured the same way over time. Consistent availability also supports accountability, escalation and evidence-based decisions, which are central themes in ISACA's governance and management guidance for monitoring performance and conformance. If the data source is not consistently available, the organization may experience gaps in reporting, delayed identification of control degradation, and reduced confidence in whether risk responses are working as intended. ISACA's COBIT resources emphasize the importance of governance and management objectives, performance monitoring and information quality in achieving enterprise objectives; see ISACA COBIT. NIST's security performance measurement guidance similarly highlights that meaningful measures require repeatable collection and reliable supporting data; see NIST SP 800-55 Rev. 1.

QUESTION NO: 177

An organization is preparing to transfer a large number of customer service representatives to the sales department. Of the following, who is responsible for mitigating the risk associated with residual system access?

A. IT service desk manager

B. Sales manager

C. Customer service manager

D. Access control manager

ANSWER: C

Explanation:

The Customer service manager is correct because residual system access in this scenario relates to access the representatives already have from their current customer service roles. Under ISACA-aligned risk governance principles, accountability for mitigating access-related risk belongs to the business owner or risk owner for the process and information being protected, not merely to the technical function that processes access changes. The customer service manager is best positioned to identify which customer service privileges are no longer justified, confirm that those privileges are removed as part of the transfer, and ensure access remains aligned with least privilege and business need. ISACA's glossary describes a risk owner as the person or function accountable for managing a risk, which fits the manager responsible for the affected business area and its information assets: ISACA Glossary. This also aligns with account management control practices such as reviewing accounts and modifying or disabling access when users are transferred, as described in NIST SP 800-53 control AC-2: NIST SP 800-53 Rev. 5.

QUESTION NO: 178

Which of the following control detects problem before it can occur?

A. Deterrent control

B. Detective control

C. Compensation control

D. Preventative control

ANSWER: D

Explanation:

Preventative control is correct because this type of control is designed to act before an unwanted event, error, or risk event materializes. In an IS risk and control environment, preventative controls are implemented to stop or reduce the likelihood of a problem by identifying risky conditions early and enforcing rules before processing continues. Examples include access restrictions, input validation, segregation of duties, configuration baselines, approval requirements, and automated edit checks. These controls may "detect" warning signs or invalid conditions in advance, but their key purpose is to prevent the problem from occurring rather than merely reporting it afterward. This aligns with the CRISC risk response and control design perspective: controls should be selected and operated based on how they reduce risk likelihood and/or impact, and preventative controls primarily reduce likelihood by blocking or correcting risky activity at the front end. For additional context on control design and risk management practices, see ISACA's CRISC credential overview at ISACA CRISC and NIST's control catalog guidance at NIST SP 800-53 Rev. 5.

QUESTION NO: 179

A maturity model is MOST useful to an organization when it:

A. benchmarks against other organizations

B. defines a qualitative measure of risk

C. provides a reference for progress

D. provides risk metrics.

ANSWER: C

Explanation:

The correct answer is “provides a reference for progress.” A maturity model is most valuable because it gives an organization a structured way to understand its current level of capability, define a desired future level, and measure improvement over time. In an ISACA/COBIT context, maturity or capability concepts are commonly used to support continual improvement by showing where processes, controls, or risk practices stand today and what must be improved to reach target outcomes. This makes the model a practical management tool: it helps stakeholders compare the current state against an agreed scale, identify gaps, prioritize improvement initiatives, and track whether those initiatives are producing measurable advancement. The core usefulness is not the score itself, but the shared reference point it creates for planning and monitoring progress. ISACA’s COBIT materials emphasize governance and management objectives supported by performance and capability considerations, which align with this improvement-oriented use of maturity models. See ISACA COBIT resources and the CMMI Institute maturity level overview for related maturity and capability model concepts.

QUESTION NO: 180

The PRIMARY objective for selecting risk response options is to:

A. minimize residual risk.

B. reduce risk factors.

C. reduce risk to an acceptable level.

D. identify compensating controls.

ANSWER: C

Explanation:

The correct answer is **reduce risk to an acceptable level.** In CRISC and ISACA risk management practice, selecting a risk response is not about eliminating risk completely; it is about choosing an appropriate response that brings the risk within the organization’s defined risk appetite and tolerance. Once risk has been identified and analyzed, management evaluates possible responses such as mitigation, avoidance, transfer or sharing, and acceptance. The primary goal of that selection is to ensure the remaining level of risk is acceptable to the business and aligned with enterprise objectives, regulatory expectations, and stakeholder requirements.

This wording is important because risk decisions are business decisions. A response may still leave residual risk, but that residual risk is acceptable if it falls within approved thresholds and is consciously accepted by accountable management. ISACA materials consistently frame governance and risk management around value delivery, risk optimization, and alignment with enterprise objectives, as reflected in COBIT. ISACA’s glossary also reinforces the use of risk-related terms such as risk appetite and residual risk in this context. Therefore, the best primary objective is to reduce risk to an acceptable level.

QUESTION NO: 181

Which of the following control is used to ensure that users have the rights and permissions they need to perform their jobs, and no more?

A. System and Communications protection control

B. Audit and Accountability control

C. Access control

D. Identification and Authentication control

ANSWER: C

Explanation:

Access control is correct because it is the control area responsible for limiting what authenticated users, processes, and systems are allowed to do after access has been granted. In risk and control practice, this includes assigning permissions based on business need, enforcing authorization rules, and regularly ensuring that access remains appropriate for the user's role. The key principle reflected in the question is least privilege: users should receive only the minimum rights needed to perform assigned job duties, and no additional access that could increase the likelihood or impact of misuse, error, or compromise.

This aligns with recognized control guidance such as the NIST SP 800-53 Access Control family, which includes controls for account management, access enforcement, separation of duties, and least privilege. In particular, least privilege is explicitly addressed as a mechanism to restrict access to only authorized functions and information necessary for users or processes. These practices directly support CRISC risk management objectives by reducing excessive access risk and helping ensure that permissions remain aligned with business responsibilities. See NIST SP 800-53 Revision 5 and NIST Risk Management Framework.