ISACA.CISA.v2026-06-30.q305

Exam Code:	CISA
Exam Name:	Certified Information Systems Auditor
Certification Provider:	ISACA
Free Question Number:	305
Version:	v2026-06-30
# of views:	103
# of Questions views:	3050
https://www.freecram.net/torrent/ISACA.CISA.v2026-06-30.q305.html	

NEW QUESTION: 1
When reviewing IT asset life cycle management within an organization, it is MOST important for the IS auditor to confirm each asset has been assigned:
A. a value
B. a security label
C. a location
D. an owner
Answer: D (LEAVE A REPLY)
The most important factor when reviewing IT asset life cycle management is confirming that each asset has been assigned an owner. An owner is responsible for the proper management, security, and maintenance of the asset throughout its lifecycle. This ensures accountability for the asset, including its usage, updates, and eventual disposal or decommissioning.

NEW QUESTION: 2
The PRIMARY purpose of a vulnerability assessment in a cybersecurity program is to:
A. Enhance the security awareness of employees and other internal stakeholders.
B. Identify known security exposures before attackers find them.
C. Improve the overall security posture of the organization.
D. Protect the organization's IT assets against external cyberthreats.
Answer: (SHOW ANSWER)
The primary purpose of vulnerability assessments is to identify known weaknesses before they can be exploited by attackers.
Option A: Security awareness is a benefit but not the main purpose.
Option C: Improving posture is an outcome, not the direct purpose.
Option D: Protection against threats is broader than vulnerability assessment.

NEW QUESTION: 3

Which of the following should be of GREATEST concern to an IS auditor reviewing onsite preventive maintenance for an organization's business-critical server hardware?
A. Preventive maintenance costs exceed the business's allocated budget
B. Preventive maintenance is outsourced to multiple vendors without requiring nondisclosure agreements (NDAs)
C. The preventive maintenance schedule is based on mean time between failures (MTBF) parameters
D. Preventive maintenance has not been approved by the information system owner
Answer: (SHOW ANSWER)
The greatest concern for an IS auditor would be if preventive maintenance has not been approved by the information system owner. Approval from the system owner ensures that the maintenance aligns with the organization's risk management and operational needs, and any unapproved changes could introduce unforeseen risks or vulnerabilities to business-critical systems.

NEW QUESTION: 4
When an organization conducts business process improvements, the IS auditor should be MOST concerned with the:
A. adequacy of reporting to senior management
B. lack of version control over process documentation
C. adequacy of the controls in the redesigned process
D. metrics used to evaluate key operating segments
Answer: (SHOW ANSWER)
When an organization undergoes business process improvements, changes to the processes can introduce new risks or weaken existing controls. The primary concern of the IS auditor should be ensuring that the redesigned process includes adequate controls to mitigate risks, maintain compliance, and protect the integrity, confidentiality, and availability of information systems. While reporting to senior management, version control, and metrics are important aspects, the adequacy of controls in the redesigned process is crucial for maintaining the security and reliability of the business operations after the improvements.

NEW QUESTION: 5
What should an IS auditor do FIRST when a follow-up audit reveals some management action plans have not been initiated?
A. Provide a report to the audit committee
B. Escalate the lack of plan completion to executive management
C. Confirm whether the identified risks are still valid
D. Request an additional action plan review to confirm the findings
Answer: (SHOW ANSWER)
Before escalating the issue or taking further action, the auditor should first confirm whether the risks that prompted the original action plans are still relevant or if circumstances have changed.

This ensures that any subsequent actions, such as reporting to the audit committee or escalating to executive management, are based on accurate and current risk assessments.
If the risks are still valid, then further actions like escalation or reporting may be necessary, but confirming the risk is a critical first step.

NEW QUESTION: 6
Which of the following is the BEST way to detect unauthorized copies of licensed software on systems?
A. Require senior management approval when installing licenses
B. Conduct periodic software scanning
C. Perform periodic counting of licenses
D. Implement controls to prohibit downloads of unauthorized software
Answer: (SHOW ANSWER)
Conducting periodic software scanning is the best way to detect unauthorized copies of licensed software. It allows for regular identification of unlicensed or unauthorized software installations on systems, ensuring compliance and helping to avoid legal and security risks.

NEW QUESTION: 7
What would be an IS auditor's BEST recommendation upon discovering that customer records in a database have not been protected?
A. Encrypt the data in the database.
B. Perform periodic access reviews.
C. Ensure database patches are installed.
D. Implement audit logging.
Answer: (SHOW ANSWER)
Encrypting the data in the database provides the most effective protection for customer records by ensuring confidentiality even if unauthorized access occurs, directly addressing the lack of data protection at rest.

NEW QUESTION: 8
Which of the following is MOST important to consider when determining the usefulness of audit evidence?
A. Nature of evidence gathered
B. Competence of the IS auditor
C. Timing of the evidence
D. Overall objectives of the review
Answer: (SHOW ANSWER)
The usefulness of audit evidence is primarily determined by how well it aligns with the overall objectives of the review. Evidence must be relevant, reliable, and sufficient to support conclusions that address the audit's goals and scope effectively.

NEW QUESTION: 9
Which of the following is the MOST important requirement in an organization's incident management response plan?
A. Escalation procedures
B. Incident reporting templates
C. Board approvals
D. Key performance indicators (KPIs)
Answer: (SHOW ANSWER)
Escalation procedures are essential to ensure incidents are promptly communicated to the appropriate levels of management and response teams, enabling timely decision-making, containment, and mitigation of impact.

NEW QUESTION: 10
During the review of a system disruption incident, an IS auditor notes that IT support staff were put in a position to make decisions beyond their level of authority. Which of the following is the BEST recommendation to help prevent this situation in the future?

A. Implement fallback options.
B. Enable an emergency access ID.
C. Develop a competency matrix.
D. Introduce escalation protocols.
Answer: D (LEAVE A REPLY)
Escalation protocols clearly define when and how decisions must be passed to higher levels of authority during incidents, preventing support staff from making decisions beyond their assigned authority and ensuring appropriate management involvement.

NEW QUESTION: 11
Which of the following is the MOST important consideration when defining the recovery time objective (RTO) for a business-critical system?
A. Maximum acceptable data loss
B. Backup of data and configurations
C. Customer and business uptime requirements
D. Supporting infrastructure
Answer: (SHOW ANSWER)
The recovery time objective (RTO) defines the maximum allowable downtime for a business-critical system before significant business impact occurs. Therefore, it must be aligned with the customer and business uptime requirements, as these directly reflect the organization's operational and service-level expectations. Meeting these requirements ensures minimal disruption to business processes and customer satisfaction.

NEW QUESTION: 12

A healthcare organization is implementing internet of Things (IoT) technology to receive customer health information from medical service providers at the point of data creation. Which of the following is the MOST important element to include in the audit plan?

A. Compliance to privacy legislation

B. Technology compatibility

C. Disaster recovery plan (DRP) for the system

D. System response times

Answer: (SHOW ANSWER)

Given the sensitivity of health information and the stringent regulations around the protection of personal data (such as HIPAA in the U.S. or GDPR in Europe), ensuring compliance with privacy legislation is critical. The healthcare sector must ensure that IoT systems collecting and transmitting health data adhere to data protection laws to safeguard patient privacy and avoid legal penalties.

While technology compatibility, disaster recovery, and system response times are important considerations, the most pressing concern in this context is compliance with privacy regulations due to the handling of sensitive personal health information.

NEW QUESTION: 13

An objective of capacity management is to ensure that:

A. organizational resources are used efficiently

B. available resources are fully utilized

C. resource utilization does not drop below 85%

D. new resources are allocated for new applications

Answer: (SHOW ANSWER)

The objective of capacity management is to ensure that organizational resources are used efficiently. This involves balancing the available capacity with current and future demands, ensuring that resources are neither underutilized nor overstrained, thereby optimizing performance and costs.

NEW QUESTION: 14

Vulnerability identification should begin in which phase of an in-house software development project?

A. Development phase

B. Design phase

C. Requirements definition phase

D. Implementation phase

Answer: (SHOW ANSWER)

Vulnerability identification should begin in the design phase of an in-house software development project. Identifying and addressing security concerns early in the design phase helps mitigate risks before the development and implementation phases, reducing the chances of vulnerabilities being introduced later in the process.

NEW QUESTION: 15
What is the MAIN reason to use incremental backups?
A. To increase backup resiliency and redundancy
B. To reduce costs associates with backups
C. To minimize the backup time and resources
D. To improve key availability metrics
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
When auditing an organization's implementation of Zero Trust principles within its identity and access management (IAM) framework, which of the following is MOST important to review for alignment?
A. Information security policies
B. The organization's core business capabilities
C. The annual IT assurance universe
D. User account management processes
Answer: A (LEAVE A REPLY)
When auditing Zero Trust implementation, the IS auditor should first ensure that the organization's information security policies align with Zero Trust principles - such as continuous verification, least privilege, and explicit trust based on identity and context. These policies form the foundation for consistent enforcement across the IAM framework.

NEW QUESTION: 17
An organization is using Internet of Things (IoT) technology to support its business processes. Which of the following is the BEST approach for the use of IoT to ensure compliance with standard information security procedures?
A. Reset passwords for default IoT device accounts.
B. Hard-code credentials into applications.
C. Evaluate IoT device vendors based on their usability.
D. Integrate the IoT network with the organizational network.
Answer: (SHOW ANSWER)

Changing default passwords on IoT devices is a fundamental security control that aligns with standard information security procedures. Default credentials are widely known and often exploited, so resetting them significantly reduces the risk of unauthorized access to IoT devices and networks.

NEW QUESTION: 18
Effective separation of duties in an online environment can BEST be achieved by utilizing:
A. appropriate supervision.
B. access authorization tables.
C. written procedure manuals.
D. transaction logging.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
What is the PRIMARY purpose of documenting audit objectives when preparing for an engagement?
A. To help ensure maximum use of audit resources during the engagement
B. To address the overall risk associated with the activity under review
C. To identify areas with relatively high probability of material problems
D. To help prioritize and schedule auditee meetings
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which of the following approaches will ensure recovery time objectives (RTOs) are met for an organization's disaster recovery plan (DRP)?

A. Performing a parallel test
B. Performing a cyber-resilience test
C. Performing a tabletop test
D. Performing a full interruption test
Answer: (SHOW ANSWER)

NEW QUESTION: 21
An organization that has decided to approve the use of end-user computing (EUC) should FIRST ensure:
A. EUC use cases are assessed and documented.
B. an EUC policy is developed.
C. a business impact analysis (BIA) is conducted.
D. EUC controls are reviewed.
Answer: (SHOW ANSWER)

NEW QUESTION: 22

Which of the following MOST effectively enables consistency across high-volume software changes?

A. Publication of a refreshed policy on development and release management

B. Management reviews of detailed exception reports for released code

C. The use of continuous integration and deployment pipelines

D. An ongoing awareness campaign for software deployment best practices

Answer: C (LEAVE A REPLY)

Continuous integration and deployment (CI/CD) pipelines automate the processes of building, testing, and deploying code, ensuring consistency, reliability, and efficiency across high-volume software changes. These pipelines minimize human error, enforce standardized processes, and provide immediate feedback, making them the most effective method for achieving consistency in software development and release.

NEW QUESTION: 23

Which of the following environments is BEST used for copying data and transformation into a compatible data warehouse format?

A. Testing

B. Replication

C. Staging

D. Development

Answer: (SHOW ANSWER)

NEW QUESTION: 24

The charging method that effectively encourages the MOST efficient use of IS resources is:

A. residual income in excess of actual incurred costs

B. allocations based on the ability to absorb charges

C. specific charges that can be tied back to specific usage

D. total utilization to achieve full operating capacity

Answer: (SHOW ANSWER)

The most efficient way to encourage the use of IS resources is by applying specific charges that can be directly tied to specific usage. This approach provides clear incentives for users to optimize their use of resources, as they are directly charged based on how much they consume. This method promotes accountability and cost-efficiency in resource utilization.

NEW QUESTION: 25

When an intrusion into an organization's network is detected, which of the following should be done FIRST?

A. Identify nodes that have been compromised.

B. Notify senior management

C. Contact law enforcement.

D. Block all compromised network nodes.

Answer: (SHOW ANSWER)

NEW QUESTION: 26
Which of the following is the MOST effective control for discovering unauthorized cloud service usage in a corporate network?
A. Reviewing firewall logs
B. Monitoring any credit card or other payments for cloud services
C. Reviewing queries to the internal domain name system (DNS) servers
D. Conducting regular software audits
Answer: (SHOW ANSWER)
The most effective control for discovering unauthorized cloud service usage in a corporate network is reviewing firewall logs. These logs can reveal outgoing traffic to cloud services and identify any unauthorized connections or data transfers to external cloud providers, helping to detect unauthorized cloud service usage.

NEW QUESTION: 27
A global company has been using a publicly available AI tool to obtain information about global laws and regulations that could impact the business. Which of the following should be of MOST concern to an IS auditor?
A. Accuracy and quality of the data provided by the AI tool
B. Whether the organization is using a paid version of the AI tool
C. Version and provider of the AI tool being utilized
D. Whether the tool is utilized by competitors in the same industry
Answer: (SHOW ANSWER)
The biggest risk is reliance on inaccurate or low-quality legal/regulatory information, which could result in compliance failures. Other concerns (paid tier, provider, competitors) are secondary.

NEW QUESTION: 28
An organization using a cloud provider for its online billing system requires the website to be accessible to customers at all times. What is the BEST way to verify the organization's business requirements are met?
A. Agree on periodic performance discussions with the vendor
B. Monitor the service level agreement (SLA) with the vendor.
C. Invoke the right-to-audit clause.
D. Require the vendor to report any outages longer than five minutes
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which of the following is MOST important for an IS auditor to ensure when evaluating an organization's end-user computing (EUC) policy as part of an IT governance audit?
A. The EUC policy supports business objectives.

B. The EUC policy identifies control procedures.
C. The EUC policy requires signed acknowledgment by users.
D. The EUC policy is covered in onboarding and awareness training.
Answer: (SHOW ANSWER)
The most important aspect for an IS auditor to verify is that the end-user computing (EUC) policy defines appropriate control procedures - such as data validation, access management, version control, and backup requirements. These controls are essential to mitigate risks associated with user-developed applications and ensure data integrity and compliance.

NEW QUESTION: 30
Which of the following is the PRIMARY function of a data loss prevention (DLP) policy when implemented in an organization's DLP solution?

A. To encrypt sensitive data at rest and in transit
B. To define rules for monitoring and protecting sensitive data
C. To define rules and baselines for network performance
D. To detect and block incoming network traffic
Answer: (SHOW ANSWER)
A DLP policy's primary purpose is to establish the criteria (rules) that determine what constitutes sensitive information and specify how that data should be monitored, handled, or blocked. This policy framework drives all detection and protection actions within the DLP solution.

NEW QUESTION: 31
Which of the following should be of GREATEST concern to an IS auditor reviewing project documentation for a client relationship management (CRM) system migration project?
A. Employees are concerned that data representation in the new system is completely different from the old system.
B. The technical migration is planned for a holiday weekend and end users may not be available.
C. A single implementation phase is planned and the legacy system will be immediately decommissioned.
D. Five weeks prior to the target date, there are still numerous defects in the printing functionality.
Answer: (SHOW ANSWER)

NEW QUESTION: 32

Which of the following IT service management activities is MOST likely to help with identifying the root cause of repeated instances of Network latency?

A. Incident management

B. Configuration management

C. Change management

D. Problem management

Answer: (SHOW ANSWER)

NEW QUESTION: 33

An IS auditor is reviewing how password resets are performed for users working remotely. Which type of documentation should be requested to understand the detailed steps required for this activity?

A. Guidelines

B. Policies

C. Procedures

D. Standards

Answer: (SHOW ANSWER)

Procedures provide detailed, step-by-step instructions for specific activities, such as password resets for remote users. They describe how tasks should be carried out in a consistent and secure manner, making them the appropriate documentation for understanding the exact steps involved in the password reset process.

NEW QUESTION: 34

An auditee has informed the IS auditor that there is not enough funding to implement an agreed-upon recommendation in the audit report and that there is no estimated time frame for resolution. What is the BEST way for the auditor to respond to this situation?

A. Obtain internal audit approval to remove the finding from the report

B. Make a recommendation to increase the IT budget

C. Assess the risk given the full solution cannot be implemented

D. Close the finding and note the auditee's explanation

Answer: (SHOW ANSWER)

In this scenario, it is essential for the IS auditor to reassess the risk that remains due to the lack of funding for the recommended solution. The auditor should evaluate whether the risk is significant enough to require further action or if alternative, lower-cost mitigations can be implemented. This helps ensure that the organization is still aware of and managing the risk, even if the full recommendation cannot be implemented at this time.

Removing the finding or closing it without proper risk assessment would not be appropriate, as the risk may remain unaddressed. Recommending an increase in the IT budget may not be feasible or within the auditor's purview. Therefore, reassessing the risk is the most prudent response.

NEW QUESTION: 35
Which of the following controls should an IS auditor recommend for a small organization where a single employee performs the combined functions of server operator and application programmer?
A. Require approval on all change requests prior to deployment.
B. Hire additional technical staff in order to force separation of duties.
C. Implement automated logging and monitoring of changes made to development libraries.
D. Implement automated controls to prevent the operator logon ID from making program modifications.
Answer: (SHOW ANSWER)
Automated logging and monitoring of changes made to development libraries provides compensating control when separation of duties is not feasible, enabling management and auditors to detect unauthorized or inappropriate changes performed by the individual with combined responsibilities.

NEW QUESTION: 36
Which of the following BEST ensures that effective change management is in place in an IS environment?
A. Adequate testing was carried out by the development team.
B. User authorization procedures for application access are well established.
C. Access to production source and object programs is well controlled.
D. User-prepared detailed test criteria for acceptance testing of the software.
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which of the following should be the GREATEST concern to an IS auditor evaluating an organization's policies?
A. Policies are not reviewed by the chief information officer (CIO).
B. Policies do not identify adequate controls or processes to protect the organization.
C. Policies are not updated on an annual basis.
D. Policies are not formally acknowledged and signed by employees.
Answer: (SHOW ANSWER)
The greatest concern is the lack of clear guidance on controls or processes because policies exist to establish expectations and protect the organization. Without adequate controls defined, policies fail to provide the necessary framework to manage risks, leaving the organization vulnerable.

NEW QUESTION: 38
Which of the following approaches would utilize data analytics to facilitate the testing of a new account creation process?
A. Review the business requirements document for date of birth field requirements.
B. Attempt to submit new account applications with invalid dates of birth

C. Evaluate configuration settings for the date of birth field requirements.
D. Review new account applications submitted in the past month for invalid dates of birth
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
An organization is concerned about duplicate vendor payments on a complex system with a high volume of transactions. Which of the following would be MOST helpful to an IS auditor to determine whether duplicate vendor payments exist?
A. Stratified sampling
B. Computer-assisted technique
C. Process walk-through
D. Statistical sampling
Answer: (SHOW ANSWER)
A computer-assisted audit technique (CAAT) enables the IS auditor to analyze large volumes of transaction data efficiently to identify potential duplicate vendor payments by comparing key fields such as vendor ID, invoice number, and amount. This automated approach is the most effective for detecting duplicates in high-volume, complex systems.

NEW QUESTION: 40
Nonrepudiation services for e-commerce transactions is BEST achieved through which of the following?
A. Transport Layer Security (TLS)
B. Message authentication code
C. Public key infrastructure (PKI)
D. Data Encryption Standard (DES)
Answer: (SHOW ANSWER)
Public key infrastructure (PKI) provides nonrepudiation by using digital signatures that verify the sender's identity and ensure that a transaction cannot later be denied. This mechanism establishes trust and accountability in e-commerce transactions.

NEW QUESTION: 41
When auditing a virtual IT system, it is MOST important to verify the security of which of the following?
A. Virtual machines (VMs)
B. Workloads
C. Hypervisor
D. Management console
Answer: (SHOW ANSWER)
The hypervisor is the core software layer that manages and controls the virtual machines (VMs) in a virtualized environment. If the hypervisor is compromised, all the VMs running on it could also be at risk. Securing the hypervisor is crucial for ensuring the overall security and integrity of the virtual environment.

While securing virtual machines, workloads, and the management console are important, the hypervisor is the foundation of the entire virtualization infrastructure. A vulnerability or breach at the hypervisor level can have widespread consequences across the entire virtual environment.

NEW QUESTION: 42
Which of the following is the BEST disposal method for flash drives that previously stored confidential data?
A. Overwriting
B. Destruction
C. Degaussing
D. Cryptographic erasure
Answer: (SHOW ANSWER)

NEW QUESTION: 43
Which of the following should be the MOST important consideration when determining which information system application to audit?
A. Available resources
B. Cost-benefit analysis
C. Newly implemented systems
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)
A business impact analysis identifies the criticality of systems and their effect on business operations. When deciding which applications to audit, the BIA provides the most important input because it helps prioritize systems based on their importance to the organization and the potential impact of failure or compromise.

NEW QUESTION: 44
An organization uses public key infrastructure (PKI) to provide email security. Which of the following would be the MOST efficient method to determine whether email messages have been modified in transit?
A. The message is sent along with an encrypted hash of the message.
B. The message is encrypted using a symmetric algorithm.
C. The message is encrypted using the private key of the sender.
D. The message is sent using Transport Layer Security (TLS) protocol.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which of the following threats is mitigated by a firewall?
A. Intrusion attack
B. Passive assault
C. Trojan horse

D. Asynchronous attack
Answer: (SHOW ANSWER)

NEW QUESTION: 46
Which of the following responsibilities associated with a disaster recovery plan (DRP) can be outsourced to a Disaster Recovery as a Service (DRaaS) provider?
A. Stakeholder communications during a disaster
B. System recovery procedures
C. Processes for maintaining currency of data
D. Validation of recovered data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 47
Which of the following is the MOST important control consideration when planning the audit of an information system that uses a large language model?
A. The alignment of model outputs with business continuity plans (BCPs)
B. The effectiveness of logical access controls over the model's training data
C. The frequency of physical security checks at the data center hosting the model
D. The schedule for the maintenance of the hardware used by the model
Answer: B (LEAVE A REPLY)
Logical access controls over the model's training data are the most important consideration because unauthorized access or manipulation of training data can directly compromise the integrity, confidentiality, and reliability of the large language model's outputs, leading to biased, inaccurate, or noncompliant results.

NEW QUESTION: 48
Which of the following is the MOST important consideration when implementing a Zero Trust strategy for mobile, wireless, and Internet of Things (IoT) devices?
A. Validating the identity of all devices and users before granting access to resources
B. Focusing on user training and awareness to prevent phishing attacks
C. Implementing strong encryption protocols for data in transit and at rest
D. Ensuring the latest firmware updates are applied regularly to all devices
Answer: (SHOW ANSWER)

The core principle of a Zero Trust strategy is "never trust, always verify." Therefore, continuously validating the identity and security posture of all users and devices - especially mobile, wireless, and IoT devices - before granting access is the most critical consideration to maintain a secure Zero Trust environment.

NEW QUESTION: 49

Which of the following is MOST useful for determining the appropriate system recovery time?

A. Key risk indicators (KRIs)

B. Service level agreement (SLA)

C. Recovery point objective (RPO)

D. Business impact analysis (BIA)

Answer: (SHOW ANSWER)

A business impact analysis (BIA) identifies the criticality of business processes and quantifies the potential impact of downtime. It provides the necessary input for determining appropriate recovery time objectives (RTOs), ensuring that system recovery aligns with business needs and continuity requirements.

NEW QUESTION: 50

An organization's email service is hosted by a third party, and the service level agreement (SLA) requires 99.9% availability. An IS auditor finds that the service has not met its availability level for the past five months. Which of the following is the auditor's BEST recommendation?

A. Self-host an email server and monitor availability.

B. Withhold payment until availability service level is met.

C. Review the service provider relationship and consider alternatives.

D. Discontinue use of the email service provider.

Answer: (SHOW ANSWER)

When a third-party service provider consistently fails to meet SLA requirements, the IS auditor should recommend reviewing the relationship to assess root causes, evaluate contractual remedies, and consider alternative providers if necessary. This ensures continuity of service and accountability without making premature operational or financial decisions.

NEW QUESTION: 51

Which of the following BEST describes the concept of fault tolerance in system resiliency?

A. It enables switching to redundant systems in case of faults.

B. It minimizes downtime and ensures continuous operations.

C. It allows systems to continue operating in the presence of faults.

D. It distributes workloads across multiple servers to prevent overload.

Answer: (SHOW ANSWER)

Fault tolerance refers to the ability of a system to continue functioning despite the occurrence of faults or hardware failures.

Option A: Describes failover, not fault tolerance.

Option B: Is a benefit but not the exact definition.
Option D: Refers to load balancing, not fault tolerance.

NEW QUESTION: 52
Which of the following is the MOST likely outcome for an organization that implements cloud computing?
A. Outsourced services for all IT operations
B. Reduced hardware spending
C. Unlimited free storage
D. Limited need for skilled IT staff
Answer: (SHOW ANSWER)
Cloud computing allows organizations to reduce their reliance on on-premises hardware by leveraging the infrastructure of cloud service providers. This reduces the need for significant capital expenditure on hardware, as computing resources (e.g., servers, storage) are provided as a service and can be scaled as needed.
While cloud computing may involve outsourcing some IT operations, it typically doesn't mean outsourcing all IT services. Storage is generally not free, and while the need for certain IT roles may change, skilled IT staff are still required for managing cloud environments, security, and application deployment.

NEW QUESTION: 53
Which of the following would provide the BEST evidence that a cloud provider's change management process is effective?
A. Minutes from regular change management meetings with the vendor
B. Written assurances from the vendor's CEO and CIO
C. The results of a third-party review provided by the vendor
D. A copy of change management policies provided by the vendor
Answer: (SHOW ANSWER)
The results of a third-party review provided by the vendor would provide the best evidence that a cloud provider's change management process is effective, because it would be an independent and objective assessment of the vendor's compliance with best practices and standards for managing changes in the cloud environment. A third-party review would also include testing of the vendor's change management controls and procedures, and provide recommendations for improvement if needed.
Minutes from regular change management meetings with the vendor would not provide sufficient evidence, because they would only reflect the vendor's self-reported information and may not capture all the changes that occurred or their impact on the cloud services. Written assurances from the vendor's CEO and CIO would also not provide sufficient evidence, because they would be based on the vendor's own opinion and may not be verified by external sources. A copy of change management policies provided by the vendor would not provide sufficient evidence,

because it would only show the vendor's intended approach to change management, but not how it is implemented or monitored in practice.

NEW QUESTION: 54
When selecting a new data loss prevention (DLP) solution, the MOST important consideration is that the solution:
A. is cost effective and meets proposed return on investment (ROI) criteria
B. provides comprehensive reporting and alerting features with detailed insights on data movements
C. is compatible with legacy IT infrastructure and integrates with other security tools
D. identifies and safeguards confidential information from unauthorized transmission
Answer: (SHOW ANSWER)
The fundamental goal of any DLP solution is to accurately discover sensitive data and enforce controls that prevent its unauthorized disclosure. All other features - cost, reporting, and integration - are secondary to ensuring the tool reliably detects and protects confidential information.

NEW QUESTION: 55
Outsourcing the development of business systems is MOST likely to result in the loss of:
A. responsibility for IT security.
B. accountability for end products.
C. control over strategic direction.
D. in-house competencies.
Answer: (SHOW ANSWER)
Outsourcing system development most commonly results in the loss of in-house competencies because knowledge, technical skills, and experience are transferred to the external provider, reducing the organization's internal capability to independently develop, maintain, or enhance systems.

NEW QUESTION: 56
Which of the following is a PRIMARY benefit of having an IS auditor facilitate control self-assessments (CSAs) with business employees?
A. It decreases employee workload through one-time reviews
B. It compensates for the need to have business stakeholder ownership of internal controls
C. It helps to support employee awareness of risks to the business
D. It provides employees with control over business processes
Answer: (SHOW ANSWER)
The primary benefit of having an IS auditor facilitate control self-assessments (CSAs) with business employees is that it helps support employee awareness of risks to the business. Through the CSA process, employees are actively engaged in identifying, assessing, and addressing risks and controls, which enhances their understanding of potential threats and their

role in mitigating those risks. This improves the overall risk management culture within the organization.

NEW QUESTION: 57
Which of the following is the PRIMARY objective of cyber resiliency?
A. To efficiently and effectively recover from an incident with limited operational impact
B. To resume normal operations after service disruptions
C. To prevent potential attacks or disruptions in operations
D. To limit the severity of security breaches and maintain continuous operations
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Which of the following would be MOST important to include in an IS audit report?
A. The roadmap for addressing the various risk areas
B. Specific technology solutions for each audit observation
C. Observations not reported as findings due to inadequate evidence
D. The level of unmitigated risk along with business impact
Answer: (SHOW ANSWER)

NEW QUESTION: 59
An IS auditor reviewing database security should be MOST concerned if the database administrator (DBA):
A. approves access roles
B. resolves database locks
C. executes recovery procedures
D. assesses database performance
Answer: (SHOW ANSWER)
Allowing the DBA to both manage the database and approve user access roles concentrates too much power in one role. This violates the principle of segregation of duties and increases the risk of unauthorized or inappropriate access going undetected.

NEW QUESTION: 60
How does the emergence of quantum computing impact traditional data encryption methods?
A. Quantum computing may render classical encryption algorithms obsolete due to its ability to decrypt data with unprecedented efficiency.
B. Quantum computing introduces new encryption techniques that are immune to decryption by classical and quantum computers alike.
C. Quantum computing enhances the security of classical encryption algorithms by providing faster computation speeds.
D. Quantum computing will require more frequent training on the application of classical data encryption methods.

Answer: (SHOW ANSWER)
Quantum algorithms, such as Shor's algorithm, can factor large prime numbers exponentially faster than classical computers, threatening the security of RSA and elliptic-curve cryptography. Similarly, Grover's algorithm reduces the effective strength of symmetric key algorithms by half, requiring larger key sizes. While post-quantum cryptography is being developed, current algorithms may become obsolete once practical quantum computers exist. Options B, C, and D are incorrect because quantum does not inherently improve encryption, nor is training the key issue-it is the fundamental breakage of cryptographic assumptions.

NEW QUESTION: 61
An organization is implementing a new cloud-based application to store sensitive customer data. The application is hosted in a country with a different regulatory environment than the organization's home country. Which of the following is the BEST way to ensure data compliance with regulatory requirements?
A. Confirm the cloud provider's teams of service are compliant with the organization's regulatory requirements
B. Review the cloud provider's infrastructure details and control documentation
C. Implement data security to protect from unauthorized access in line with local regulatory requirements
D. Review the cloud provider's logs for any signs of unauthorized access or misuse
Answer: (SHOW ANSWER)
The best way to ensure data compliance with regulatory requirements is to review the cloud provider's infrastructure details and control documentation. This ensures that the cloud provider implements the necessary controls and complies with relevant regulations, including those concerning data storage, protection, and privacy. This is particularly important when the application is hosted in a jurisdiction with a different regulatory environment, as it allows the organization to verify that the provider's policies align with the organization's compliance obligations.

NEW QUESTION: 62
In an effort to use transaction log resources effectively and free up space, an organization has decided to begin truncating older log information. Which of the following is MOST important to ensure?

A. Approval has been obtained from the data owner before the truncation is performed
B. The database server has been rebooted in the past month
C. Transactions in progress are rolled back after the truncation is complete
D. A schedule for periodic truncation has been established
Answer: (SHOW ANSWER)
The most important consideration is obtaining approval from the data owner before truncating older log information. This ensures that the data owner is aware of and agrees to the truncation process, preventing the accidental loss of critical data or violating data retention policies. Proper authorization is essential to maintain data integrity and compliance with legal or regulatory requirements.

NEW QUESTION: 63
Which of the following should be an IS auditor's GREATEST concern when assessing an IT service configuration database?
A. The database is write-accessible for all users.
B. The database is executable for all users.
C. The database is read-accessible for all users.
D. The database is not encrypted at rest.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
An IS auditor is reviewing a contract for the outsourcing of IT facilities. If missing, which of the following should present the GREATEST concern to the auditor?
A. Access control requirements
B. Perimeter network security diagram
C. Help desk availability
D. Hardware configurations
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which of the following are examples of corrective controls?
A. Implementing separation of duties and hash totals
B. Performing internal audit reviews and remediation activities
C. Applying rollback scripts and backup procedures
D. Enforcing disciplinary action and termination procedures
Answer: (SHOW ANSWER)
Corrective controls are measures taken to restore systems or processes after an incident or error has occurred.
Option C: Rollback scripts and backup procedures restore systems, making them corrective controls.
Option A: Separation of duties and hash totals are preventive controls.

Option B: Audit reviews are detective, while remediation may include corrective, but audits themselves aren't corrective.
Option D: Disciplinary actions are deterrent controls.

NEW QUESTION: 66
An IS auditor is supporting a forensic investigation. An image of affected storage media has been captured while collecting digital forensic evidence. Which of the following techniques would BEST enable an IS auditor to verify that the captured image is an exact, unchanged replica of the original media?
A. File allocation table
B. Hash value
C. Access control list
D. Size of the file
Answer: (SHOW ANSWER)
A hash value is a cryptographic checksum generated by applying a hash function (e.g., SHA-256 or MD5) to the data. If the hash value of the captured image matches the hash value of the original media, it confirms that the image is an exact, unchanged replica. Hashing is a widely accepted forensic technique to ensure data integrity during investigations.
The file allocation table, access control list, and file size do not provide the same level of assurance regarding the exactness of the data replication as hashing does.

NEW QUESTION: 67
Which of the following should be of GREATEST concern to an IS auditor reviewing security standards implemented in an organization?
A. The baseline security standards differ across applications.
B. The baseline security standards for operating systems are not uniform.
C. The baseline security standards lack guidelines on patching.
D. The baseline security standards are at a generic level.
Answer: (SHOW ANSWER)
Missing patch management guidelines represent the greatest concern because unpatched systems are a leading cause of security breaches. Without clear patching requirements, systems may remain vulnerable to known exploits, undermining the effectiveness of the organization's entire security posture.

NEW QUESTION: 68
Which of the following application should an IS auditor consider to be the HIGHEST priority when reviewing disaster recovery planning (DRP) tests for an e-commerce company?
A. An application for financial management
B. An application for traffic load balancing
C. An application for IT performance monitoring
D. An application for HR management

Answer: (SHOW ANSWER)

The highest priority for an IS auditor when reviewing disaster recovery planning (DRP) tests for an e-commerce company should be an application for financial management. This is because financial transactions, payments, and accounting are critical to the business's revenue and operations. Any downtime or failure in this area could have severe financial and legal consequences, making it the most critical application to ensure recovery procedures are in place and tested effectively.

NEW QUESTION: 69

Which of the following would provide the MOST useful information for evaluating whether network availability is meeting the performance objectives set by management?

A. Metrics dashboard

B. Capability maturity model

C. IT value analysis

D. Gap analysis

Answer: (SHOW ANSWER)

A metrics dashboard provides real-time, quantifiable data on network performance and availability. It allows the IS auditor or management to directly compare actual performance against defined objectives, making it the most useful tool for evaluating whether availability targets are being met.

NEW QUESTION: 70

An IS auditor is reviewing the quality control (QC) of the implementation process that supports an online reservation system. Which of the following findings would be the GREATEST concern?

A. Use of compensating manual controls in place of systemic controls

B. Lack of business sign-off for technical configuration and settings

C. Lack of a peer review process during user acceptance testing (UAT) cycles

D. Inadequate process to identify and control defects

Answer: (SHOW ANSWER)

The greatest concern in this scenario would be an inadequate process to identify and control defects. Without a proper process in place to detect, track, and address defects during the implementation of the online reservation system, the system could experience errors, vulnerabilities, or performance issues that could impact functionality, user experience, and security. Proper defect management is essential to ensure the system operates as intended and meets quality standards.

NEW QUESTION: 71

Data restoration tests the effectiveness of an organization's ability to:

A. verify whether data can be replicated to multiple sites.

B. test the implementation of data backup technology.

C. verify whether encrypted data on tapes can be recovered with minimal loss.

D. reliably retrieve data should the need arise.

Answer: D (LEAVE A REPLY)

The primary purpose of data restoration testing is to confirm that backed-up data can be successfully and reliably recovered when needed, ensuring business continuity and data availability in the event of data loss or system failure.

NEW QUESTION: 72

Which of the following is the PRIMARY objective of data loss prevention (DLP) mechanisms?

A. Enhancing system performance while safeguarding against data loss

B. Automating data loss recovery procedures to minimize downtime in case of incidents

C. Protecting against unauthorized transmissions or disclosure of sensitive data

D. Ensuring compliance with regulatory requirements for data protection

Answer: (SHOW ANSWER)

The central goal of DLP is to prevent sensitive data-such as PII, PHI, or intellectual property-from leaving the organization through unauthorized channels. DLP solutions monitor, detect, and block potential data exfiltration via email, endpoints, cloud applications, or removable media. While compliance (D) is often a driver, it is a secondary outcome of implementing DLP. Enhancing performance (A) and recovery automation (B) are not objectives of DLP. ISACA positions DLP as a critical control for confidentiality under DSS05 (Managed Security Services).

NEW QUESTION: 73

After a functional change to a program in a system, regression testing of the system is important in order to check whether the:

A. change has adversely affected that system

B. changed program performs as specified by the new program design

C. changed program performs efficiently and effectively

D. changed program functions as required by the user specifications for the change

Answer: (SHOW ANSWER)

Regression testing is primarily important to ensure that the recent functional change has not adversely affected other parts of the system. It helps verify that previously working features of the system continue to function correctly and that the new change does not introduce new defects or issues in other areas of the system.

NEW QUESTION: 74

Which of the following performance management tools BEST helps an IS auditor evaluate the success of an organization's IT strategy implementation and execution?

A. IT benchmarking

B. Capability maturity model

C. Six Sigma

D. IT metrics dashboard

Answer: (SHOW ANSWER)

An IT metrics dashboard provides real-time monitoring and reporting on key IT performance indicators (KPIs), allowing auditors and management to evaluate the effectiveness of IT strategy implementation and execution.
Option A (Benchmarking): Useful for comparisons with peers but not for ongoing execution.
Option B (Maturity models): Assess long-term process maturity, not direct strategy execution.
Option C (Six Sigma): Focuses on process improvement, not IT strategy monitoring.
Option D: Correct - dashboards link strategy to measurable outcomes.

NEW QUESTION: 75
Which of the following BEST enables an IS auditor to assess whether jobs were completed according to the job schedule?
A. Console log
B. Exception log
C. System schedule
D. Database schedule
Answer: (SHOW ANSWER)
The console log records the execution of jobs, including details about job start and completion times, errors, and other runtime information. By reviewing the console log, an IS auditor can verify whether jobs were executed as per the schedule and identify any issues or irregularities in their execution.
While the system schedule and database schedule outline when jobs are supposed to run, and the exception log captures any errors or exceptions, the console log provides the actual records of job executions, making it the most reliable source to verify job completion against the schedule.

NEW QUESTION: 76
Which of the following is the PRIMARY role of key performance indicators (KPIs) in supporting business process effectiveness?
A. To evaluate the cost-benefit of tools implemented to monitor control performance
B. To enable conclusions about the performance of the processes and target variances for follow-up analysis
C. To analyze workflows in order to optimize business processes and eliminate tasks that do not provide value
D. To assess the functionality of a software deliverable based on business processes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 77
Which of the following should be done FIRST when planning to conduct internal and external penetration testing for a client?
A. Identify milestones.
B. Establish the timing of testing.
C. Establish the rules of engagement.
D. Determine the test reporting.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Which of the following is the PRIMARY role of the IT steering committee?
A. Facilitating collaboration between business and IT
B. Granting authorization for periodic IT audits
C. Periodically reporting to business units about IT performance
D. Ensuring business units are supporting IT objectives
Answer: (SHOW ANSWER)
The primary role of the IT steering committee is to facilitate collaboration between business and IT. This ensures that IT initiatives are aligned with the business strategy, fostering communication and coordination to achieve organizational objectives.

NEW QUESTION: 79
An organization is implementing a new data loss prevention (DLP) tool. Which of the following will BEST enable the organization to reduce false positive alerts?
A. Configuring a limited set of rules
B. Using the default policy and tool rule sets
C. Deploying the tool in monitor mode
D. Reducing the number of detection points
Answer: (SHOW ANSWER)

NEW QUESTION: 80
What should be the PRIMARY focus during a review of a business process improvement project?
A. The cost of new controls
B. Continuous monitoring plans
C. Business impact
D. Business project plan
Answer: (SHOW ANSWER)

NEW QUESTION: 81

An IS auditor is reviewing a decision to consolidate processing for multiple applications onto a single large server. Which of the following is the MOST significant impact from this decision?
A. Fewer application servers requiring vulnerability scans
B. Higher operating system license fees
C. Simplified asset management
D. More applications affected by a server outage
Answer: (SHOW ANSWER)
Consolidating multiple applications onto a single large server increases the dependency on that server. If the server experiences a failure or outage, all applications hosted on it will be impacted simultaneously, resulting in broader system downtime and business disruption. This represents the most significant impact compared to cost or administrative changes.

NEW QUESTION: 82
Which of the following should be done FIRST following an incident that has caused internal servers to be inaccessible, disrupting normal business operations?
A. Make a bit-level copy of the affected servers and calculate the hash value of the copy.
B. Copy all key directories and files on the affected servers and generate the hash value of the copy.
C. Unplug all power cables immediately to prevent further actions of the attacker on the servers.
D. Document the servers' dates, times, and locations, as well as the individual who last used them.
Answer: (SHOW ANSWER)
Creating a bit-level copy (also known as a forensic image) of the affected servers and calculating the hash value ensures that an exact replica of the system is preserved for forensic analysis without altering the original data. This is critical for investigating the incident, understanding what happened, and maintaining the integrity of the evidence. The hash value guarantees that the copy remains unchanged and can be used as evidence if needed.
While documenting the servers and their usage, copying directories, and even unplugging the servers could be necessary steps later, preserving the system's state through a forensic copy is the top priority to avoid data loss or contamination.

NEW QUESTION: 83
Which of the following is the BEST metric to measure the quality of software developed in an organization?
A. Amount of successfully migrated software changes
B. Reduction in the help desk budget
C. Number of defects discovered in production
D. Increase in quality assurance (QA) activities
Answer: C (LEAVE A REPLY)
https://getdx.com/blog/software-quality-metrics/

NEW QUESTION: 84
Following a breach, what is the BEST source to determine the maximum amount of time before customers must be notified that their personal information may have been compromised?
A. Industry standards
B. Information security policy
C. Incident response plan
D. Industry regulations
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Which of the following scenarios poses the GREATEST security concern during the system development life cycle (SDLC)?
A. Rolling out internet-facing servers to the production environment with vendor default settings
B. Engaging a third-party vendor for code development and testing in the cloud environment
C. Using ar open source library to support certain web application functionalities
D. Remediating critical and high-risk findings after web application scanning
Answer: (SHOW ANSWER)
Internet-facing servers with vendor default settings are a significant security risk because default configurations, including default usernames, passwords, and open ports, are often well-known and easily exploited by attackers. This can expose the servers to unauthorized access and attacks, such as brute force attacks or malware infections, putting the entire system at risk. While the other scenarios (third-party vendor engagement, using open source libraries, and remediating vulnerabilities) also pose risks, the immediate and potentially severe exposure of production servers with default settings is the greatest concern. Attackers could exploit these vulnerabilities quickly and compromise critical systems.

NEW QUESTION: 86
An organization uses an automated continuous integration/continuous deployment (CI/CD) tool to deploy changes to production. Which of the following would be an IS auditor's GREATEST concern in this situation?
A. Releases are scheduled once per week.
B. Post-implementation reviews are conducted quarterly.
C. Test cases may be inaccurate.
D. Functional requirements are changed frequently by users.
Answer: (SHOW ANSWER)
The greatest concern in a CI/CD environment is the accuracy of automated testing. Since code is deployed rapidly and often without manual intervention, weak or inaccurate test cases can allow vulnerabilities and defects to be pushed directly into production. Release frequency (A) and changing user requirements (D) are expected characteristics of agile/DevOps models and can be managed with governance. Delayed post-implementation reviews (B) may reduce oversight but do not directly undermine the core pipeline integrity. ISACA's DevOps guidance emphasizes that

automated testing and validation of requirements must be thorough and reliable to ensure continuous deployment does not compromise quality or security.

NEW QUESTION: 87
Which of the following testing methods is MOST appropriate for assessing whether system integrity has been maintained after changes have been made?
A. Regression testing
B. Integration testing
C. Acceptance testing
D. Unit testing
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following would be of MOST concern to an IS auditor reviewing a data loss prevention (DLP) solution implementation for endpoints?
A. The solution does not prevent data leakage because it is still in the monitoring phase.
B. The organization has never finished tuning the solution.
C. The DLP solution does not support all types of servers.
D. The solution has been implemented in blocking mode prior to performing tuning.
Answer: (SHOW ANSWER)
Implementing a DLP solution in blocking mode before adequate tuning creates a high risk of false positives that can disrupt business operations, block legitimate data transfers, and negatively impact productivity, indicating ineffective and risky deployment practices.

NEW QUESTION: 89
Which of the following should be done FIRST to ensure that a data loss prevention (DLP) process is appropriately implemented?
A. Determine methods used to transmit data
B. Classify the data stored on its systems
C. Identify the locations of the data on its systems
D. Measure the volume of data stored
Answer: B (LEAVE A REPLY)
The first step in implementing a data loss prevention (DLP) process is to classify the data stored on the systems. Understanding the types of data, their sensitivity, and how they should be protected is essential before establishing controls, monitoring, and prevention mechanisms.

NEW QUESTION: 90
Which of the following should be the PRIMARY consideration when reviewing console logs to access the effectiveness of an organization's job scheduling process?

A. Verifying whether are authorized to assign or change job schedules and priorities
B. Determining whether the jobs ran and were completed according to schedule

C. Evaluating whether the scheduling procedures facilitate optimal use of computer resources
D. Confirming whether operators record all exception processing requests
Answer: (SHOW ANSWER)
The primary consideration when reviewing console logs to assess the effectiveness of an organization's job scheduling process is determining whether the jobs ran and were completed according to schedule. This ensures that the job scheduling process is functioning as intended, with tasks being executed on time and without disruptions, which is crucial for maintaining operational efficiency and meeting business deadlines.

NEW QUESTION: 91
Which of the following responses to risk associated with separation of duties would incur the LOWEST initial cost?
A. Risk transference
B. Risk reduction
C. Risk mitigation
D. Risk acceptance
Answer: (SHOW ANSWER)
Accepting the risk involves acknowledging its existence without taking immediate action to mitigate, transfer, or reduce it. This approach incurs the lowest initial cost because no additional controls, insurance, or resources are implemented upfront.

NEW QUESTION: 92
An IS auditor is reviewing the service management of an outsourced help desk. Which of the following is the BEST indicator of how effectively the service provider is performing this function?
A. Customer satisfaction ratings
B. Call transcript reviews
C. Average ticket age
D. Number of calls worked
Answer: (SHOW ANSWER)

NEW QUESTION: 93
Which of the following is the GREATEST concern associated with IS risk-based auditing when audit resources are limited?

A. There may be significant delays in responding to management audit requests
B. Some business processes may not be audited
C. Conducting risk assessments may reduce the time available for auditing
D. The audit schedule may become too predictable
Answer: (SHOW ANSWER)
The greatest concern with IS risk-based auditing when audit resources are limited is that some business processes may not be audited. Focusing on high-risk areas may leave other potentially important processes unexamined, leading to gaps in the audit coverage and missed opportunities to identify risks in less critical areas.

NEW QUESTION: 94
An organization has experienced frequent of malware exploiting vulnerabilities to its network. Which of the following would be an IS auditor's BEST recommendation to address this issue?
A. Stateful inspection firewall
B. Demilitarized zone (DMZ)
C. Continuous port scanning
D. Intrusion prevention system (IPS)
Answer: (SHOW ANSWER)
An Intrusion Prevention System (IPS) is the best recommendation to address malware exploiting vulnerabilities, as it actively monitors network traffic for malicious activity and prevents it in real-time. Unlike passive solutions, an IPS can block malicious payloads and prevent vulnerabilities from being exploited, providing an effective defense against frequent malware attacks.

NEW QUESTION: 95
Which of the following concerns is MOST effectively addressed by implementing an IT framework for alignment between IT and business objectives?
A. Inadequate IT portfolio management
B. Lack of a benchmark analysis
C. Inaccurate business impact analysis (BIA)
D. Inadequate IT change management practices
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Job scheduling impacts system availability and reliability by:
A. Reducing system downtime.
B. Ensuring flexibility and scalability.
C. Optimizing resource utilization.
D. Decreasing system complexity.
Answer: (SHOW ANSWER)
Job scheduling is a core operational control that ensures workloads are executed in an orderly and efficient manner, balancing demands across processing resources. Its primary benefit is

optimization of system resources--CPU, memory, I/O, and network bandwidth--leading to improved throughput and consistent service levels. While scheduling may indirectly reduce downtime (A) or support scalability (B), its direct impact is ensuring resources are allocated efficiently. Decreasing complexity (D) is not the key purpose of scheduling. ISACA's DSS01 (Managed Operations) recognizes workload and job scheduling as crucial practices for sustaining reliable, high-performance IT services.

NEW QUESTION: 97
Which of the following components of a risk assessment is MOST helpful to management in determining the level of risk mitigation to apply?
A. Risk classification
B. Control self-assessment (CSA)
C. Impact assessment
D. Risk identification
Answer: (SHOW ANSWER)

NEW QUESTION: 98
Which of the following is the MOST important consideration to facilitate prosecution of a perpetrator after a cyber crime?
A. An active intrusion detection system (IDS)
B. Immediate law enforcement involvement
C. Professional collection of unaltered evidence
D. Reporting to the internal legal department
Answer: (SHOW ANSWER)
Ensuring evidence is gathered, preserved, and documented correctly - with its integrity and chain of custody intact - is essential for its admissibility in court and thus critical to successfully prosecuting a cyber-crime.

NEW QUESTION: 99
Which of the following BEST protects evidence in a forensic investigation?
A. Powering down the affected system
B. Rebooting the affected system
C. Protecting the hardware of the affected system
D. Imaging the affected system
Answer: (SHOW ANSWER)

NEW QUESTION: 100
During a database security audit, an IS auditor is reviewing the process used to input data. Which of the following is the MOST significant risk area for the auditor to focus on?

A. Data resilience
B. Data availability

C. Data normalization
D. Data integrity
Answer: (SHOW ANSWER)
The key audit concern at data input is integrity-ensuring accuracy, validity, and completeness. Without integrity, outputs cannot be trusted. Availability and resilience are operational concerns, while normalization is a design technique. Integrity remains the top security and audit focus.

NEW QUESTION: 101
Which of the following computer forensics activities allows the examination of information that is only available on active operating system processes?
A. Disk imaging and analysis
B. Antimalware log analysis
C. Primary memory imaging and analysis
D. Firmware dumping and analysis
Answer: (SHOW ANSWER)
Primary memory imaging and analysis allow the examination of information that is only available on active operating system processes. This type of analysis captures the contents of RAM, which can include valuable information such as running processes, encryption keys, and other transient data that is not stored on disk.

NEW QUESTION: 102
An IS auditor is reviewing an organization's business continuity plan (BCP) following a change in organizational structure with significant impact to business processes. Which of the following findings should be the auditor's GREATEST concern?
A. Key business process end users did not participate in the business impact analysis (BIA).
B. A call tree exercise has not been completed in the last two years.
C. Copies of the BCP have not been distributed to new business unit end users since the reorganization.
D. The most recent business impact analysis (BIA) was performed two years before the reorganization.
Answer: (SHOW ANSWER)
A business impact analysis (BIA) must reflect the current organizational structure and business processes. Since the reorganization significantly changed operations, relying on an outdated BIA means that critical processes, dependencies, and recovery priorities may no longer be accurate - posing the greatest risk to business continuity effectiveness.

NEW QUESTION: 103
Which of the following is a core functionality of a configuration and release management system?
A. Identifying other configuration items that will be impacted by a given change
B. Managing privileged access to databases, servers, and infrastructure
C. Identifying vulnerabilities in configuration settings

D. Deploying a configuration change to the sandbox environment
Answer: (SHOW ANSWER)

NEW QUESTION: 104
When testing the accuracy of transaction data, which of the following situations BEST justifies the use of a smaller sample size?
A. It is expected that the population is error-free.
B. Proper separation of duties is in place.
C. The data can be directly changed by users.
D. The IS audit staff has a high level of experience
Answer: (SHOW ANSWER)

NEW QUESTION: 105
What is the main objective when implementing security controls within an application?
A. To optimize user functionality of the application
B. To optimize the level of data protection achieved against cost
C. To minimize reputational risk to the organization
D. To minimize the exposure to the fullest extent possible
Answer: (SHOW ANSWER)
The main objective of implementing security controls within an application is to balance effective data protection with cost efficiency. Controls should provide adequate security proportional to the value and sensitivity of the data without incurring unnecessary expense or complexity.

NEW QUESTION: 106
An IS auditor discovers that due to resource constraints, a database administrator (DBA) is responsible for developing and executing changes Into the production environment. Which of the following should the auditor do FIRST?
A. Determine whether another database administrator (DBA) could make the changes.
B. Identify whether any compensating controls exist.
C. Report a potential segregation of duties (SoD) violation
D. Ensure a change management process is followed prior to implementation.
Answer: (SHOW ANSWER)

NEW QUESTION: 107
A small startup organization does not have the resources to implement separation of duties. Which of the following is the MOST effective compensating control?
A. Mandatory vacations
B. Additional management reviews and reconciliations
C. Third-party assessments
D. Rotation of log monitoring and analysis responsibilities
Answer: B (LEAVE A REPLY)
When separation of duties cannot be implemented due to limited resources, enhanced management reviews and reconciliations serve as the most effective compensating control. These reviews provide oversight and independent verification of activities, reducing the risk of undetected errors or fraud.

NEW QUESTION: 108
An organization has decided to reengineer business processes to improve the performance of overall IT service delivery. Which of the following recommendations from the project team should be the GREATEST concern to the IS auditor?
A. Disable operational logging to enhance the processing speed and save storage.
B. Adopt a service delivery model based on insights from peer organizations.
C. Eliminate certain reports and key performance indicators (KPIs).
D. Delegate business decisions to the chief risk officer (CRO).
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Which of the following BEST describes the role of the IS auditor in a control self-assessment (CSA)?
A. Implementer
B. Reviewer
C. Facilitator
D. Approver
Answer: (SHOW ANSWER)

NEW QUESTION: 110
Which of the following should be of GREATEST concern to an IS auditor reviewing an organization's mobile device policies and controls in its corporate environment?

A. Remote wipe and lock features are only available with access to the internet
B. Not all active devices are enrolled in mobile device management (MDM)
C. The virtual private network (VPN) policy is not enabled for the internal corporate network
D. The mobile authentication policy requires biometrics
Answer: (SHOW ANSWER)

Unmanaged devices fall outside corporate controls - lacking enforced encryption, patch management, app restrictions, remote wipe capabilities and other safeguards - making them the greatest risk for data loss, malware infection or unauthorized access.

NEW QUESTION: 111
Which of the following should be of GREATEST concern to an IS auditor when using data analytics?
A. The data analytics software is open source.
B. The data was not extracted by the auditor.
C. The data source lacks integrity.
D. The data set contains irrelevant fields.
Answer: (SHOW ANSWER)

NEW QUESTION: 112
An IS auditor is reviewing the security of corporate databases holding customer data. A decentralized model is used, and remote queries are necessary. Which of the following should be of GREATEST concern?
A. There are several public database links for remote queries.
B. Contractors have developed database links for remote queries.
C. There is a large number of database links for remote queries.
D. Performance issues were identified due to the database links for remote queries.
Answer: (SHOW ANSWER)
Public database links allow remote connections without authentication, creating a serious security vulnerability that can expose sensitive customer data. In a decentralized model with remote queries, this poses the greatest concern because it bypasses access controls and can be exploited for unauthorized data access.

NEW QUESTION: 113
The management of a small e-commerce firm is concerned about the impact of AI adoption on its intellectual property. Which of the following BEST addresses this concern?
A. Developing an AI acceptable use policy
B. Sanctioning employees for using generative AI
C. Performing manual reviews of AI web traffic logs
D. Deny-listing chat-based AI websites and plugins
Answer: (SHOW ANSWER)
The best approach is to establish a clear AI acceptable use policy that defines how employees may use AI tools while protecting sensitive information and intellectual property. This ensures governance while enabling safe adoption.
Option B: Reactive and punitive, not proactive governance.
Option C: Monitoring helps but is insufficient alone.
Option D: Overly restrictive and may block beneficial AI use.

Option A: Correct - policies provide structured guidance aligned with business objectives and risk management.

NEW QUESTION: 114
An organization is migrating its HR application to an Infrastructure as a Service (IaaS) model in a private cloud. Who is PRIMARILY responsible for the security configurations of the deployed application's operating system?
A. The cloud provider's external auditor
B. The cloud provider
C. The operating system vendor
D. The organization
Answer: (SHOW ANSWER)

NEW QUESTION: 115
A bank performed minor changes to the interest calculation computer program. Which of the following techniques would provide the STRONGEST evidence to determine whether the interest calculations are correct?
A. Manual verification of a sample of the results
B. Parallel simulation using audit software
C. Review of the quality assurance (QA) test results
D. Source code review
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which of the following would provide an organization with the BEST evidence that a third party's controls are aligned with the organization's requirements?
A. The third party's information security policies
B. Independent audit reports
C. The organization's regulatory requirements
D. Service level agreements (SLAs)
Answer: (SHOW ANSWER)
Independent audit reports provide the best evidence that a third party's controls are aligned with the organization's requirements. These reports are typically conducted by an external party and offer an objective assessment of whether the third party's controls meet the necessary security, privacy, and regulatory standards.

NEW QUESTION: 117
Which type of digital evidence is at GREATEST risk of being lost if not captured in a timely manner?
A. Text messages
B. Social media posts

C. Internet browsing history
D. Cached data
Answer: (SHOW ANSWER)
Cached data is at the greatest risk of being lost if not captured in a timely manner. Cached data is often stored temporarily on devices and can be overwritten or deleted as the system continues to operate or as space is needed. Unlike text messages, social media posts, or internet browsing history (which are typically stored more persistently), cached data can be easily lost if not captured quickly during a forensic investigation.

NEW QUESTION: 118
Which of the following is the BEST way to ensure Internet of Things (IoT) devices do not retain default admin passwords?
A. Performing configuration management throughout the asset life cycle
B. Conducting file-sharing reviews throughout the asset life cycle
C. Implementing vulnerability management throughout the asset life cycle
D. Auditing activity logs throughout the asset life cycle
Answer: (SHOW ANSWER)
Configuration management ensures that IoT devices are securely configured and maintained according to defined standards, including changing default admin passwords. Continuous configuration management throughout the asset life cycle helps prevent insecure default settings from persisting and reduces the risk of unauthorized access.

NEW QUESTION: 119
The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:
A. authorization.
B. integrity.
C. nonrepudiation.
D. authenticity.
Answer: (SHOW ANSWER)
https://fastercapital.com/content/Exploring-the-Importance-of-Checksum-in-Data-Integrity.html

NEW QUESTION: 120
An organization has alternative links in its wide area network (WAN) to provide redundancy. However, each time there is a problem with a link, network administrators have to update the configuration to divert traffic to the other link. Which of the following would be an IS auditor's BEST recommendation?

A. Reduce the number of alternative links
B. Implement a load-balancing mechanism
C. Configure a non-proprietary routing protocol
D. Implement an exterior routing protocol

Answer: C (LEAVE A REPLY)
Deploying a standards-based dynamic routing protocol (for example, OSPF) lets routers automatically discover and advertise link status. When one WAN link fails, the routing tables converge and traffic is rerouted over the backup path without manual intervention, providing seamless redundancy.

NEW QUESTION: 121
Management has decided to accept a risk in response to a draft audit recommendation. Which of the following should be the IS auditor's NEXT course of action?
A. Ensure a follow-up audit is on next year's plan.
B. Escalate the acceptance to the board.
C. Document management's acceptance in the audit report.
D. Escalate acceptance to the audit committee.
Answer: (SHOW ANSWER)
The IS auditor should record management's decision to accept the risk in the audit report, ensuring it is clearly documented. This provides transparency and accountability, noting that management has consciously decided to accept the identified risk.
Escalating the acceptance to the board or audit committee may be necessary only if the accepted risk is significantly outside the organization's risk appetite or policy. However, the first step is to document the decision. Ensuring a follow-up audit can be planned if required, but documenting the decision is the most immediate and essential action.

NEW QUESTION: 122
An IS auditor finds that firewalls are outdated and not supported by vendors. Which of the following should be the auditor's NEXT course of action?
A. Report the mitigating controls.
B. Determine the risk of not replacing the firewall.
C. Report the security posture of the organization.
D. Determine the value of the firewall.
Answer: (SHOW ANSWER)

NEW QUESTION: 123

Which of the following is the PRIMARY reason for an IT department to establish operational level agreements (OLAs) in pursuit of improving management of IT service levels?
A. To ensure service-level requirements for all internal IT functions are captured
B. To document end-user requirements for IT services
C. To ensure external providers understand service-level objectives
D. To establish adequate budget allocation for IT services across business units
Answer: (SHOW ANSWER)
Operational Level Agreements (OLAs) define the interdependent responsibilities and performance targets among internal IT teams that support overall Service Level Agreements (SLAs). Their primary purpose is to ensure that internal functions work cohesively to meet the organization's agreed service-level objectives.

NEW QUESTION: 124
If concurrent update transactions to an account are not processed properly, which of the following will be affected?
A. Accountability
B. Availability
C. Integrity
D. Confidentiality
Answer: (SHOW ANSWER)
Data integrity refers to the accuracy, consistency, and reliability of data. When concurrent transactions are not properly managed, it can lead to issues such as race conditions, data corruption, or conflicting updates, which compromise the integrity of the account information. Proper transaction handling ensures that the data remains consistent and accurate despite multiple updates happening at the same time.
Accountability, availability, and confidentiality are important as well, but improper processing of concurrent transactions directly impacts the integrity of the data.

NEW QUESTION: 125
Which of the following is the PRIMARY benefit of benchmarking an organization's software development life cycle practices against a capability maturity model?
A. Security requirements are added to software development processes.
B. Reliable products are guaranteed.
C. Programmers' efficiency is improved.
D. Repeatable software development procedures are established.
Answer: (SHOW ANSWER)
https://www.cascade.app/blog/maturity-model-overview

NEW QUESTION: 126
Which of the following is MOST important for an IS auditor to determine when reviewing the design and implementation of controls?

A. Whether there is a proper balance between the magnitude of the risk and the control measures implemented
B. Whether the implemented controls closely align with domestic and international industry best practices
C. Whether adequate resources are available for frequent and stringent control monitoring
D. Whether identified risks are being completely mitigated through the proper application of control mechanisms
Answer: A (LEAVE A REPLY)
The most important factor for an IS auditor to determine when reviewing the design and implementation of controls is whether there is a proper balance between the magnitude of the risk and the control measures implemented. Effective risk management involves aligning the level of control with the potential impact of the risk, ensuring that resources are appropriately allocated to mitigate significant risks without overburdening the organization with unnecessary controls.

NEW QUESTION: 127
Which of the following BEST enables an IS auditor to prioritize financial reporting spreadsheets for an end- user computing (EUC) audit?
A. Ascertaining which spreadsheets are most frequently used
B. Understanding the purpose of each spreadsheet
C. Reviewing spreadsheets based on file size
D. Identifying the spreadsheets with built-in macros
Answer: (SHOW ANSWER)

NEW QUESTION: 128
Which of the following is MOST important for an IS auditor to look for in a project feasibility study?
A. An assessment of whether requirements will be fully met
B. An assessment indicating security controls will operate effectively
C. An assessment indicating the benefits will exceed the investment
D. An assessment of whether the expected benefits can be achieved
Answer: (SHOW ANSWER)

NEW QUESTION: 129
Which of the following is an example of a vulnerability?
A. System outages
B. Unpatched systems
C. A malicious insider
D. An organization's reputation
Answer: (SHOW ANSWER)
A vulnerability is a weakness in a system that can be exploited by a threat. Unpatched systems represent such a weakness because missing security updates leave exploitable gaps that attackers can use to compromise the system.

NEW QUESTION: 130

An IS auditor is reviewing an AI system utilized by a healthcare organization for patient pre- diagnosis. Which of the following would pose the GREATEST concern?

A. Outdated AI knowledge base

B. Outdated AI system refinement process

C. Lack of an emergency change log

D. Lack of discretionary access control

Answer: (SHOW ANSWER)

The lack of discretionary access control is the greatest concern because unauthorized access to the AI system or its underlying data could compromise patient confidentiality, violate healthcare privacy regulations, and undermine the integrity and reliability of pre-diagnosis outcomes.

NEW QUESTION: 131

Which of the following is the PRIMARY purpose of a data loss prevention (DLP) tool?

A. Blocking transmission of confidential data

B. Analyzing data at rest

C. Establishing data classification

D. Restricting the availability of confidential data

Answer: A (LEAVE A REPLY)

DLP tools are primarily designed to monitor, detect, and prevent the unauthorized transmission of sensitive or confidential data outside of an organization. This includes preventing data leaks through various channels such as email, file transfers, or cloud services. DLP tools enforce policies to ensure that confidential data does not leave the organization or fall into the wrong hands.

While DLP tools may also analyze data at rest and assist with data classification, their primary function is to block or prevent the loss or unauthorized transfer of sensitive data.

NEW QUESTION: 132

Which type of attack poses the GREATEST risk to an organization's most sensitive data?

A. Eavesdropping attack

B. Password attack

C. Spear phishing attack

D. Insider attack

Answer: (SHOW ANSWER)

NEW QUESTION: 133

Which type of device sits on the perimeter of a corporate or home network, where it obtains a public IP address and then generates private IP addresses internally?

A. Switch

B. Intrusion prevention system (IPS)

C. Gateway
D. Router
Answer: D (LEAVE A REPLY)

NEW QUESTION: 134
Which of the following should be the PRIMARY consideration when validating a data analytic algorithm that has never been used before?
A. Increasing speed and efficiency of audit procedures
B. Confirming completeness and accuracy
C. Enhancing the design of data visualization
D. Decreasing the time for data analytics execution
Answer: (SHOW ANSWER)
When validating a data analytic algorithm that has never been used before, the primary consideration should be ensuring completeness and accuracy of the algorithm's output. This ensures that the algorithm processes data correctly, produces reliable results, and supports decision-making or audit objectives effectively. Without validated accuracy and completeness, other factors such as speed or visualization enhancements are irrelevant.

NEW QUESTION: 135
Which of the following is MOST important to define within a disaster recovery plan (DRP)?
A. Business continuity plan (BCP)
B. Roles and responsibilities for recovery team members
C. Test results for backup data restoration
D. A comprehensive list of disaster recovery scenarios and priorities
Answer: (SHOW ANSWER)

NEW QUESTION: 136
In a large organization, IT deadlines on important projects have been missed because IT resources are not prioritized properly. Which of the following is the BEST recommendation to address this problem?
A. Implement a comprehensive project scorecard.
B. Implement project portfolio management.
C. Implement an integrated resource management system.
D. Revisit the IT strategic plan.
Answer: (SHOW ANSWER)
Project portfolio management (PPM) provides a structured approach to prioritizing and managing IT projects based on strategic alignment, resource capacity, and business value. This ensures that limited IT resources are allocated effectively to the most critical and high-impact initiatives, reducing delays and improving delivery outcomes.

NEW QUESTION: 137
An organization is integrating two systems for real-time API communication. Which of the following is the BEST approach to ensure secure authentication between the two applications before going live?
A. Conduct penetration testing to identify vulnerabilities that might allow unauthenticated access.
B. Perform user acceptance testing (UAT) for user login interfaces and the user authentication mechanism.
C. Review security incident and event management (SIEM) solution logs.
D. Review firewall configuration and rules across both system environments.
Answer: A (LEAVE A REPLY)
Before enabling real-time API communication between two systems, conducting penetration testing is the best approach to ensure that the authentication mechanisms are securely implemented and resistant to bypass or exploitation. This proactive testing validates that only authorized applications can access the APIs before going live.

NEW QUESTION: 138
Which of the following would be of GREATEST concern to an is auditor reviewing continuous integration/continuous deployment (CI/CD) practices?
A. Dynamic application security testing (DAST) is not performed for every build
B. If all pipeline tests pass, changes are allowed to be deployed into production without manual review
C. The time between deployments has varied from four hours to two weeks
D. Critical security test failures within the pipeline do not stop production deployment
Answer: D (LEAVE A REPLY)
The greatest concern would be if critical security test failures within the CI/CD pipeline do not prevent deployment to production. This indicates that vulnerabilities or significant security issues could be introduced into production environments, potentially exposing the system to risks. Ensuring that critical security tests act as blocking mechanisms is essential for maintaining a secure CI/CD process.

NEW QUESTION: 139
Which of the following should be the FIRST consideration when deciding whether data should be moved to a cloud provider for storage?
A. Service level agreements (SLAs)

B. Data classification
C. Vendor cloud certification
D. Data storage costs
Answer: (SHOW ANSWER)

NEW QUESTION: 140
Well-documented incident management processes contribute MOST to the:
A. periodic rotation of IT operation staff
B. reduction of total service downtime
C. identification of security weaknesses
D. promotion of a risk-aware culture
Answer: (SHOW ANSWER)
Well-documented incident management processes contribute most to the reduction of total service downtime. By having clear, predefined procedures for identifying, managing, and resolving incidents, organizations can respond more quickly and effectively, minimizing the impact and duration of service disruptions. This helps ensure that services are restored as quickly as possible, reducing overall downtime.

NEW QUESTION: 141
Which of the following is PRIMARILY used in blockchain technology to create a distributed immutable ledger?
A. Edge computing
B. Encryption
C. Application hardening
D. Artificial intelligence (AI)
Answer: (SHOW ANSWER)
Blockchain technology uses cryptographic techniques, including encryption, to secure data, verify transactions, and ensure immutability of the ledger. Cryptographic hashing, digital signatures, and encryption ensure that once data is recorded in the blockchain, it cannot be altered or tampered with, providing a secure, distributed, and immutable record.
While edge computing, application hardening, and artificial intelligence (AI) may be relevant in other contexts, encryption is central to blockchain's security and immutability features.

NEW QUESTION: 142
How is nonrepudiation supported within a public key infrastructure (PKI) environment?
A. Through the use of private keys to decrypt data received by a user
B. Through the use of enterprise key management systems
C. Through the use of a certificate issued by a certificate authority (CA)
D. Through the use of elliptical curve cryptography on transmitted messages
Answer: (SHOW ANSWER)

In a PKI, nonrepudiation is achieved by using digital signatures, which are created using the sender's private key. The certificate issued by a certificate authority (CA) binds the public key to the individual or entity, ensuring the identity of the signer. This way, the sender cannot deny having signed the message, as only their private key could have generated the corresponding signature.
While private keys, enterprise key management systems, and specific cryptographic algorithms like elliptical curve cryptography are part of the broader security ecosystem, the primary mechanism for nonrepudiation in PKI is through digital signatures supported by certificates issued by a trusted CA.

NEW QUESTION: 143
Which of the following should be the MOST important consideration in IT portfolio management?
A. Aligning IT portfolio processes with corporate objectives
B. Increasing the budget and resources allocated for IT investments
C. Determining the opportunity cost of IT investment projects
D. Selecting IT investment projects that align with corporate strategy
Answer: (SHOW ANSWER)
The most important consideration in IT portfolio management is ensuring that all IT investments directly support and align with the organization's corporate strategy. This alignment maximizes business value, ensures resource optimization, and helps prioritize projects that contribute to strategic objectives.

NEW QUESTION: 144
An IS auditor works for a company that develops software for commercial use. Which of the following is the MOST important consideration when conducting a post-implementation review of a system recently delivered to a client?
A. The project deliverables met contractual requirements
B. The system operates as the project engineers intended
C. The project will be relevant to the client in future years
D. End users provide positive feedback
Answer: A (LEAVE A REPLY)
The most important consideration during a post-implementation review of a system recently delivered to a client is whether the project deliverables met contractual requirements. Ensuring that the system aligns with the agreed-upon specifications, features, and functionality outlined in the contract is crucial for confirming that the client received what they were promised, and it ensures compliance with contractual obligations. This also serves as the foundation for future support and maintenance agreements.

NEW QUESTION: 145
Which of the following is the BEST source of organizational direction on when to use cloud services?

A. Enterprise architecture (EA)
B. Business continuity plans (BCPs)
C. Availability requirements
D. Cloud regulations
Answer: (SHOW ANSWER)
Enterprise architecture defines the organization's technology principles, standards and guidelines, including criteria for evaluating and adopting cloud services, making it the primary directive for when to use the cloud.

NEW QUESTION: 146
When reviewing network security configurations, which of the following would pose the GREATEST risk of unauthorized access?
A. Use of personal virtual private networks (VPNs)
B. Active network ports in a conference room
C. A wireless network utilizing wired equivalent privacy (WEP) encryption
D. Weak or improperly implemented access control procedures
Answer: (SHOW ANSWER)
Weak or poorly implemented access controls present the greatest risk of unauthorized access because they can compromise the entire network, regardless of other protective measures. Strong access controls ensure that only authorized users and devices can access network resources, effectively mitigating external and internal threats.

NEW QUESTION: 147
An application programming interface (API) has recently undergone a new release, and sensitive functions are no longer restricted appropriately. Which of the following is the MOST likely reason?
A. Broken object-level authorization
B. Trojan horses
C. Portability flaws
D. Erratic version control
Answer: (SHOW ANSWER)
The most likely reason for sensitive functions no longer being restricted appropriately after a new API release is broken object-level authorization. This occurs when the API fails to properly enforce access controls, allowing unauthorized users to access or perform actions on sensitive functions or data. This is a common security vulnerability, often resulting from improperly handled access checks or missed authorization logic during the development or release of new API versions.

NEW QUESTION: 148
Which of the following BEST enables an IS auditor to rely on auditee evidence?
A. Evidence and script are both provided in an encrypted spreadsheet
B. Evidence generated from a previous audit is reused

C. Evidence is observed and obtained in the form of screenshots by the auditor
D. Evidence is generated by the organization's most senior IT administrator
Answer: (SHOW ANSWER)
The best way for an IS auditor to rely on auditee evidence is if the evidence is observed and obtained directly by the auditor, such as through screenshots. This allows the auditor to independently verify the evidence, ensuring its authenticity and integrity. Relying on evidence generated by the auditee or using evidence from prior audits introduces the risk of incomplete or unverified data.

NEW QUESTION: 149
Which of the following is an organization's BEST defense against malware?
A. Documented security procedures
B. Intrusion prevention system (IPS)
C. Security awareness training
D. Intrusion detection system (IDS)
Answer: (SHOW ANSWER)
The best defense against malware is security awareness training for employees. Human error, such as clicking on phishing links or downloading malicious attachments, is one of the primary vectors for malware infections. Educating employees about recognizing threats, following safe practices, and adhering to security policies significantly reduces the risk of malware compromising the organization.

NEW QUESTION: 150
Which of the following encryption methods offers the BEST wireless security?
A. Wired equivalent privacy (WEP)
B. Secure Sockets Layer (SSL)
C. Data encryption standard (DES)
D. Wi-Fi Protected Access 3
Answer: (SHOW ANSWER)
Wi-Fi Protected Access 3 (WPA3) provides the highest level of wireless security available, offering stronger encryption (using SAE and 192-bit security), improved protection against brute-force attacks, and enhanced authentication compared to earlier protocols like WEP or WPA2.

NEW QUESTION: 151
Which of the following technologies is BEST suited to fulfill a business requirement for nonrepudiation of business-to-business transactions with external parties without the need for a mutually trusted entry?
A. Public key infrastructure (PKI)
B. Blockchain distributed ledger
C. Artificial intelligence (AI)
D. Centralized ledger technology

Answer: (SHOW ANSWER)
Blockchain provides a decentralized, immutable ledger that records transactions transparently across multiple parties. This enables nonrepudiation because once a transaction is recorded on the blockchain, it cannot be altered or denied by any party involved. Additionally, blockchain does not require a central trusted authority, as the consensus mechanism ensures trust and verification across all participants.
While PKI is also effective for nonrepudiation, it typically involves a trusted certificate authority. Blockchain, on the other hand, eliminates the need for such an intermediary, making it ideal for scenarios where mutual trust is not required.

NEW QUESTION: 152
Which of the following would BEST help to ensure that potential security issues are considered by the development team as part of incremental changes to agile-developed software?
A. Mandate that the change analyses are documented in a standard format.
B. Include a mandatory step to analyze the security impact when making changes.
C. Assign the security risk analysis to a specially trained member of the project management office.
D. Deploy changes in a controlled environment and observe for security defects.
Answer: (SHOW ANSWER)

NEW QUESTION: 153
At the end of each business day, a business-critical application generates a report of financial transac-tions greater than a certain value, and an employee then checks these transactions for errors. What type of control is in place?
A. Deterrent
B. Detective
C. Preventive
D. Corrective
Answer: (SHOW ANSWER)

NEW QUESTION: 154
Which of the following IT service monitoring tools is MOST effective in identifying abnormal system events?

A. System network and administrative logs
B. System exception and deviation reports
C. Operator problem reports
D. Operator work schedules
Answer: (SHOW ANSWER)
System exception and deviation reports are the most effective tools for identifying abnormal events, as they highlight deviations from expected processing and performance.
Logs (A): Provide raw data but require manual review or monitoring tools.
Operator problem reports (C): Capture issues but depend on human reporting, which may miss critical events.
Operator work schedules (D): Related to staffing, not abnormal events.

NEW QUESTION: 155
An IS audit reveals that a privileged user account was used to delete some transactions from application logs. Which of the following would BEST prevent the recurrence of similar irregularities?
A. Restrict access to activity logs
B. Use write once, read many media for log data storage
C. Update and share the log retention policy
D. Disable administrative accounts that are inactive
Answer: (SHOW ANSWER)
The best way to prevent the recurrence of irregularities like privileged users deleting transactions from application logs is to restrict access to activity logs. By limiting access to only authorized personnel and implementing strong access controls, the risk of unauthorized modification or deletion of log data is reduced, ensuring the integrity and accountability of logs.

NEW QUESTION: 156
When evaluating whether the expected benefits of a project have been achieved, it is MOST important for an IS auditor to review:
A. The business case.
B. The project schedule.
C. Proposed enhancements.
D. Quality assurance (QA) results.
Answer: (SHOW ANSWER)
The business case defines the project's expected benefits, success criteria, and performance metrics. Reviewing the business case allows the auditor to assess whether the benefits identified at initiation have been realized post-implementation. The schedule (B) only tracks timeliness, not value. Proposed enhancements (C) address future improvements, not whether benefits have been delivered. QA results (D) reflect product quality but not business value. ISACA emphasizes that value delivery and benefits realization are key elements of enterprise governance of IT, aligning with COBIT's EDM02 (Ensure Benefits Delivery).

NEW QUESTION: 157
Which of the following poses the GREATEST risk to an organization when employees use public social networking sites?
A. Social engineering
B. Adverse posts about the organization
C. Cross-site scripting (XSS)
D. Copyright violations
Answer: (SHOW ANSWER)
The greatest risk posed by employees using public social networking sites is social engineering. Attackers can gather personal and organizational information from these sites to craft targeted attacks, such as phishing or pretexting, to manipulate employees into disclosing sensitive information or compromising security.

NEW QUESTION: 158
An IS auditor is reviewing job scheduling software and notes instances of delayed processing time, unexpected job interruption, and out-of-sequence job execution. Which of the following should the auditor examine FIRST to help determine the reasons for these instances?
A. System schedule
B. Job schedule
C. Exception log
D. Change log
Answer: (SHOW ANSWER)
The exception log should be examined first, as it provides detailed records of errors, failures, or anomalies in the job scheduling process. This log can help the IS auditor identify specific issues causing delayed processing times, job interruptions, or out-of-sequence execution. It offers insights into the root causes and patterns of the incidents, enabling further investigation into related controls or configurations.

NEW QUESTION: 159
An organization's IT risk assessment should include the identification of:
A. business needs
B. business process owners
C. compensating controls
D. vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 160
A local insurance company has decided to migrate an in-house accounting solution to a purchased enterprise resource planning (ERP) solution. The project is entering the user acceptance testing (UAT) phase. Which of the following would pose the GREATEST risk to the effectiveness of the UAT?

A. UAT has started before functional testing is complete
B. UAT environment is an exact copy of production data
C. UAT includes business users who were not involved with the project
D. UAT is conducted by senior management
Answer: (SHOW ANSWER)
The greatest risk to the effectiveness of the User Acceptance Testing (UAT) phase is starting UAT before functional testing is complete. Functional testing ensures that the system behaves as expected from a technical perspective. If UAT begins prematurely, there is a risk that the system may have unresolved technical issues, which could lead to incorrect testing results or missed defects, ultimately undermining the effectiveness of UAT and delaying the project.

NEW QUESTION: 161
Which of the following is the PRIMARY benefit of monitoring IT operational logs?
A. Identifying configuration flaws in operating systems
B. Generating exception reports to assess security compliance
C. Detecting processing errors in a timely manner
D. Managing the usability and capacity of IT resources
Answer: (SHOW ANSWER)
https://www.esecurityplanet.com/networks/what-is-log-monitoring/

NEW QUESTION: 162
Which of the following is MOST critical to the success of an information security program?
A. Management's commitment to information security
B. Alignment of information security with IT objectives
C. Integration of business and information security
D. User accountability for information security
Answer: (SHOW ANSWER)
Management's commitment is the foundation of a successful information security program because it ensures that security initiatives receive the necessary support, resources, and prioritization across the organization. Strong management commitment drives a security-conscious culture, ensures that policies are enforced, and aligns security efforts with organizational goals.
While aligning information security with IT objectives, integrating business and security, and ensuring user accountability are also important, they are heavily influenced by management's support and commitment to fostering a robust information security environment. Without strong backing from management, other elements of the security program may struggle to gain traction or be effectively implemented.

NEW QUESTION: 163
Following an IT audit, management has decided to accept the risk highlighted in the audit report.

Which of the following would provide the MOST assurance to the IS auditor that management is adequately balancing the needs of the business with the need to manage risk?
A. Potential impact and likelihood are adequately documented.
B. A communication plan exists for informing parties impacted by the risk.
C. Established criteria exist for accepting and approving risk.
D. Identified risk is reported into the organization's risk committee.
Answer: (SHOW ANSWER)

NEW QUESTION: 164
Which of the following should be the PRIMARY focus when configuring security settings for a cloud application's infrastructure?
A. Maximizing the scalability of the application
B. Protecting resources from unauthorized access
C. Ensuring that logs are sent to the SIEM
D. Minimizing the cost of security infrastructure
Answer: (SHOW ANSWER)
The primary focus when configuring security settings for a cloud application's infrastructure should be protecting resources from unauthorized access. This ensures that sensitive data and services are safeguarded from potential breaches, which is critical for maintaining the confidentiality, integrity, and availability of the cloud application.

NEW QUESTION: 165
A finance department has a two-year project to upgrade the enterprise resource planning (ERP) system hosting the general ledger. In year one, the system version upgrade will be applied, and in year two, business processes will be updated to implement new system functionality. Which of the following should be the PRIMARY focus of an IS auditor reviewing the second year of the implementation?
A. Sociability testing
B. User acceptance testing (UAT)
C. Data migration
D. Initial user access provisioning
Answer: (SHOW ANSWER)

NEW QUESTION: 166
Following the sale of a business division, employees will be transferred to a new organization, but they will retain access to IT equipment from the previous employer An IS auditor has recommended that both organizations agree to and document an acceptable use policy for the equipment What type of control has been recommended?
A. Detective control
B. Corrective control
C. Directive control

D. Preventive control
Answer: (SHOW ANSWER)

NEW QUESTION: 167
During a routine internal software licensing review, an IS auditor discovers instances where employees shared license keys to critical pieces of business software. Which of the following would be the auditor's BEST course of action?
A. Recommend the purchase of additional software license keys
B. Recommend the utilization of software licensing monitoring tools
C. Validate user need for shared software licenses
D. Verify whether the licensing agreement allows shared use
Answer: (SHOW ANSWER)

NEW QUESTION: 168
The use of access control lists (ACLs) is the MOST effective method to mitigate security risk for routers because they:
A. act as filters between the world and the network
B. can detect cyberattacks
C. are recommended by security standards
D. can limit Telnet and traffic from the open Internet
Answer: (SHOW ANSWER)
Access control lists (ACLs) are most effective for mitigating security risks on routers because they act as filters, controlling which traffic is allowed or denied based on predefined rules. This helps protect the internal network by blocking unauthorized or malicious traffic from the outside world while allowing legitimate traffic to pass.

NEW QUESTION: 169
During a review of an organization's IT capacity management process, an IS auditor should be MOST concerned if capacity planning:
A. omitted changes to key business systems
B. lacked input from system administrators.
C. was based on input from IT service management only.
D. was reviewed once during the previous six months.

Answer: (SHOW ANSWER)

Capacity planning that omits changes to key business systems is most concerning because it can result in insufficient resources to support critical business operations, leading to performance degradation or service outages that directly impact business objectives.

NEW QUESTION: 170

Which of the following should an IS auditor do FIRST when auditing a robotics process automation (RPA) implementation?

A. Evaluate the overall solution architecture

B. Analyze the sequence of activities performed by the robot

C. Understand the business processes automated by the robot

D. Identify the credentials used by the robot and where they are stored

Answer: (SHOW ANSWER)

Before evaluating technical aspects such as the solution architecture, sequence of activities, or credential management, it is essential to first gain a clear understanding of the business processes that the RPA solution is automating. This ensures that the auditor is aware of the context and objectives of the automation, the criticality of the processes involved, and any potential risks or control requirements. Understanding the business processes lays the foundation for a more focused and effective audit of the RPA implementation.

NEW QUESTION: 171

Which of the following is the PRIMARY objective of performing quality assurance (QA) in a system development process?

A. To ensure that expected benefits have been realized

B. To ensure the developed system meets business requirements

C. To ensure the developed system integrates well with another system

D. To help determine high-level requirements for the new system

Answer: (SHOW ANSWER)

The primary objective of quality assurance (QA) in the system development process is to ensure that the system being developed adheres to the defined business requirements and specifications. QA focuses on verifying that the final product aligns with organizational needs, is free of defects, and functions as intended, thereby ensuring the project's success.

NEW QUESTION: 172

How does an organization indicate the authenticity of its web pages for users utilizing a public key infrastructure (PKI)?

A. By including trademark logos with the organization's name and physical address

B. By purchasing digital certificates from trusted third parties

C. By creating digital certificates internally and applying a stamp of authenticity

D. By coding the page utilizing Hypertext Transmission Protocol Secure (HTTPS)

Answer: (SHOW ANSWER)

To indicate the authenticity of its web pages for users utilizing a public key infrastructure (PKI), an organization should purchase digital certificates from trusted third parties, also known as Certificate Authorities (CAs). These digital certificates verify the identity of the organization and establish trust with users accessing the site, ensuring that the communication is secure and the website is legitimate.

NEW QUESTION: 173
Which of the following is the BEST compensating control against separation of duties conflicts in new code development?
A. Post-implementation change review
B. Adding the developers to the change approval board
C. Creation of staging environments
D. A small number of people have access to deploy code
Answer: (SHOW ANSWER)
If SoD cannot be fully implemented, an independent review of changes after deployment provides assurance that inappropriate or unauthorized code has not been introduced. Other options either weaken controls or fail to provide adequate oversight.

NEW QUESTION: 174
Which of the following is a KEY attribute that differentiates statistical sampling from non-statistical sampling?
A. Appropriateness
B. Sufficiency
C. Relevance
D. Randomness
Answer: (SHOW ANSWER)
A key attribute that differentiates statistical sampling from non-statistical sampling is randomness. In statistical sampling, the selection of samples is based on random methods, ensuring that every item in the population has an equal chance of being selected. This allows for the use of mathematical techniques to quantify the sampling risk and to draw conclusions about the population. In contrast, non-statistical sampling does not rely on random selection, and the samples are chosen based on judgment or other non-random criteria.

NEW QUESTION: 175
An organization is enhancing the security of a client-facing web application following a proposal to acquire personal information for a business purpose. Which of the following is MOST important to review before implementing this initiative?
A. Encryption capabilities
B. Data ownership assignments
C. Regulatory compliance requirements
D. Customer notification procedures

Answer: (SHOW ANSWER)

NEW QUESTION: 176
Storing backup drives at an offsite location is an example of which type of control?
A. Preventive
B. Detective
C. Directive
D. Administrative
Answer: (SHOW ANSWER)
Storing backup drives at an offsite location is a preventive control because it reduces the likelihood of data loss by protecting backups from site-specific risks such as fire, flooding, or other disasters affecting the primary location.

NEW QUESTION: 177
An organization has determined that a trusted insider has been able to bypass and embezzle organizational funds. Which type of audit would be MOST helpful when providing evidence to law enforcement?
A. Forensic audit
B. Integrated audit
C. Financial audit
D. Regulatory audit
Answer: (SHOW ANSWER)
A forensic audit is specifically designed to investigate fraud, embezzlement, or other financial misconduct. It involves detailed evidence collection and analysis, which is crucial for providing proof to law enforcement.

NEW QUESTION: 178
The MOST significant reason for using ley performance indicators (KPIs) to track the progress of IT projects against their initial targets is that they:
A. provide timely indication of when corrective actions need to be taken
B. influence management decisions to outsource IT projects
C. identify instances where increased stakeholder engagement is required
D. identify which projects may require additional funding
Answer: (SHOW ANSWER)
The most significant reason for using key performance indicators (KPIs) is that they provide timely indications of when corrective actions need to be taken. KPIs help track the progress of IT projects against their targets, enabling the project team and management to address issues early and keep the project on track.

NEW QUESTION: 179

An IS auditor is assessing backup performance and observes that the system administrator manually initiates backups during unexpected peak usage. Which of the following is the auditor's BEST course of action?

A. Inspect logs to verify timely execution of backups.

B. Verify the load balancer configuration.

C. Recommend using cloud-based backups.

D. Review separation of duties documentation.

Answer: A (LEAVE A REPLY)

The IS auditor's best course of action is to review backup logs to confirm whether backups are executed on schedule and completed successfully. This provides objective evidence of whether manual initiation during peak usage affects backup performance, data integrity, or recovery capability.

NEW QUESTION: 180

Which of the following is MOST important for an IS auditor to recommend when corporate mobile devices are being replaced?

A. Verify that technical specifications are identical on the old and new devices.

B. Securely transfer organizational data on old devices.

C. Ensure the teams handling the replacements have security clearance.

D. Remove old devices from the asset inventory after being replaced.

Answer: (SHOW ANSWER)

The most important consideration when replacing corporate mobile devices is ensuring that organizational data is securely transferred (and removed from old devices). This prevents data loss or unauthorized access, maintaining the confidentiality and integrity of corporate information during the replacement process.

NEW QUESTION: 181

An IS auditor is reviewing a machine learning model that predicts the likelihood that a user will watch a certain movie. Which of the following would be of GREATEST concern to the auditor?

A. The data set for training the model was obtained from an unreliable source

B. When the model was tested with data drawn from a different population, the accuracy decreased

C. An open source programming language was used to develop the model

D. The model was tested with data drawn from the same population as the training data

Answer: (SHOW ANSWER)

The quality and reliability of the training data are crucial for the model's accuracy and overall performance. If the training data comes from an unreliable source, the model's predictions could be biased, inaccurate, or unreliable, leading to poor outcomes when applied to real-world scenarios. Ensuring the integrity, quality, and reliability of the training data is fundamental for any machine learning model.

While decreased accuracy when tested with data from a different population, the use of open-source programming languages, and testing with data from the same population are important factors to consider, the reliability of the training data is the most critical issue because it directly affects the model's ability to learn correctly and generalize to new data.

NEW QUESTION: 182
Which type of security testing is MOST efficient for finding hidden errors in software and facilitating source code optimization?
A. User acceptance testing (UAT)
B. White box testing
C. Penetration testing
D. Black box testing
Answer: (SHOW ANSWER)
White box testing leverages full access to the application's source code and internal architecture, enabling testers to systematically uncover hidden logic errors, security flaws, and inefficiencies and to recommend code-level optimizations.

NEW QUESTION: 183
Which of the following should be of GREATEST concern to an IS auditor conducting an audit of an organization that recently experienced a ransomware attack?
A. Antivirus software was unable to prevent the attack even though it was properly updated.
B. Backups were only performed within the local network.
C. The most recent security patches were not tested prior to implementation.
D. Employees were not trained on cybersecurity policies and procedures.
Answer: (SHOW ANSWER)

NEW QUESTION: 184
Which of the following is the BEST way for the auditor to ensure an organization has taken adequate steps to mitigate the risk of employees exfiltrating proprietary information?
A. Review the organization's business continuity plan (BCP).
B. Verify whether the organization records log files.
C. Validate that a data loss prevention (DLP) solution was implemented.
D. Examine whether the organization's proprietary information was appropriately labeled.

Answer: (SHOW ANSWER)
A DLP solution is specifically designed to monitor, detect, and prevent unauthorized data transfers, including the exfiltration of proprietary information by employees. It can enforce policies to block or alert on attempts to move sensitive data outside the organization's control, whether through email, cloud storage, or external devices. Validating the implementation of a DLP solution provides assurance that mechanisms are in place to prevent and detect data exfiltration.
While reviewing log files, ensuring proper information labeling, and examining the business continuity plan (BCP) are important, a DLP solution directly addresses the risk of data exfiltration by employees.

NEW QUESTION: 185
Which of the following documents should define roles and responsibilities within an IT audit organization?
A. Audit scope letter
B. Annual audit plan
C. Audit charter
D. Engagement letter
Answer: (SHOW ANSWER)
The audit charter is the document that should define roles and responsibilities within an IT audit organization. It outlines the purpose, authority, and responsibilities of the audit function, ensuring that there is clarity on the scope of the audit team's duties and their alignment with the organization's objectives.

NEW QUESTION: 186
When reviewing the monitoring and prevention of sensitive data moving out of an organization's network, which of the following is MOST important for an IS auditor to verify?
A. Transport Layer Security (TLS) is used
B. Firewall rules have been documented
C. Deep packet inspection is enabled
D. Chain of custody is followed
Answer: (SHOW ANSWER)
Deep packet inspection provides the ability to examine packet payloads for sensitive content (not just headers), enabling detection and blocking of confidential data in motion. Without DPI, encrypted or non-standard traffic could bypass perimeter controls, undermining any monitoring or prevention efforts.

NEW QUESTION: 187
After areas have been appropriately scoped, what is the IS auditor's NEXT step in the selection for sampling?
A. Define the population for sampling
B. Calculate the sample size

C. Pull the sample
D. Determine the sampling method
Answer: (SHOW ANSWER)
After areas have been appropriately scoped, the next step is to define the population for sampling. This involves identifying the entire set of data or items from which the sample will be drawn, ensuring that the sample accurately represents the population being audited.

NEW QUESTION: 188
A bank wants to outsource a system to a cloud provider residing in another country. Which of the following would be the MOST appropriate IS audit recommendation?
A. Find an alternative provider in the bank's home country.
B. Ensure the provider's internal control system meets bank requirements.
C. Proceed as intended, as the provider has to observe all laws of the clients' countries.
D. Ensure the provider has disaster recovery capability.
Answer: (SHOW ANSWER)

NEW QUESTION: 189
The PRIMARY objective of the disaster recovery planning process is to:
A. comply with regulatory requirements
B. ensure data can be recovered completely
C. minimize the operational interruption
D. align incident response time with industry best practices
Answer: (SHOW ANSWER)
The core goal of disaster recovery planning is to restore critical operations as quickly as possible after a disruption, thereby minimizing downtime and its impact on the business. All other activities - data recovery, compliance, response times - support this primary aim of reducing operational interruption.

NEW QUESTION: 190
A database administrator (DBA) should be prevented from:
A. using an emergency user ID.
B. having access to production files.
C. having end user responsibilities.
D. accessing sensitive information.
Answer: (SHOW ANSWER)

NEW QUESTION: 191
Which of the following provides the BEST assurance of data integrity after file transfers?
A. Monetary unit sampling
B. Check digits
C. Hash values

D. Reasonableness check
Answer: (SHOW ANSWER)

NEW QUESTION: 192
Which of the following is the BEST compensating control to apply when hardware and software associated with a legacy system cannot be patched or updated to protect against known vulnerabilities or malware?
A. Deploy firewalls with deep packet inspection capability that can monitor and block advanced threats
B. Block all USB access to the local area network (LAN) and permit no external connections
C. Overhaul the manufacturing facility and associated IT infrastructure to ensure upgrades can be performed
D. Take down the production facility to upgrade all the infrastructure following extensive testing
Answer: (SHOW ANSWER)
Deploying firewalls with deep packet inspection (DPI) allows for thorough monitoring and filtering of traffic at a granular level, helping to detect and block malicious traffic before it can exploit vulnerabilities in unpatched legacy systems. This compensating control adds a robust layer of security by analyzing traffic and preventing known threats from reaching the vulnerable systems. While blocking USB access or overhauling/upgrading infrastructure may improve security, these options may not be practical or feasible, especially in environments with critical legacy systems. Taking down the production facility is highly disruptive and could result in significant downtime, so it is not the best compensating control. DPI-enabled firewalls provide protection without requiring major disruptions to operations.

NEW QUESTION: 193
An IS auditor is examining cryptographic key management with a focus on ensuring the protection of cryptographic keys against modification and unauthorized disclosure. Which of the following should be reviewed FIRST?
A. Key storage
B. Key rotation
C. Key generation
D. Key policies
Answer: (SHOW ANSWER)
Key management policies should be reviewed first because they define how cryptographic keys are generated, stored, distributed, used, rotated, and destroyed. Reviewing these policies establishes whether appropriate governance and controls exist to prevent unauthorized disclosure or modification of keys before assessing technical implementations.

NEW QUESTION: 194
Which of the following should be an IS auditor's PRIMARY area of focus when auditing an organization's deployment of Internet of Things (IoT) devices?

A. Interoperability of IoT devices with various brands and types
B. Energy consumption rates of the IoT devices
C. Frequency at which the IoT devices transmit data
D. Data protection measures within the IoT devices
Answer: (SHOW ANSWER)
The primary focus when auditing IoT deployments should be on data protection measures, as IoT devices often collect and transmit sensitive information. Ensuring proper encryption, authentication, and secure communication helps prevent data breaches and unauthorized access.

NEW QUESTION: 195
Which of the following is an IS auditor's BEST recommendation after identifying that HR staff create new employees in the payroll system as well as process payroll due to limited staffing?
A. Implement a payroll system user awareness training program.
B. Rotate payroll responsibilities within HR.
C. Document roles and responsibilities of payroll staff.
D. Implement independent periodic review of payroll transactions.
Answer: D (LEAVE A REPLY)
When separation of duties cannot be enforced due to limited staffing, the best compensating control is an independent periodic review of payroll transactions. This oversight helps detect and prevent errors or fraudulent activities by providing an external check on payroll processing.

NEW QUESTION: 196
Which of the following is the MOST important consideration to ensure the integrity of encrypted data?
A. The frequency of encryption key updates
B. The accessibility of decryption keys
C. The strength of the encryption algorithm
D. The establishment of an encryption policy
Answer: C (LEAVE A REPLY)
The integrity of encrypted data depends primarily on the strength of the encryption algorithm. A strong algorithm ensures that the data cannot be altered or deciphered without authorization, maintaining both confidentiality and integrity against cryptographic attacks.

NEW QUESTION: 197
Which of the following approaches BEST enables an IS auditor to detect security vulnerabilities within an application?
A. Threat modelling
B. Threat intelligence
C. Concept mapping
D. Prototyping
Answer: (SHOW ANSWER)
Threat modeling is the best approach for detecting security vulnerabilities within an application. It involves identifying potential threats, vulnerabilities, and attack vectors during the design and development stages, allowing for proactive mitigation of risks and strengthening application security.

NEW QUESTION: 198
An IS auditor is planning an implementation review of a new accounting system. Which of the following is MOST important to include in this review?
A. Data conversion results
B. Benefits realization
C. Database configurations
D. System security training
Answer: (SHOW ANSWER)
In an implementation review of a new accounting system, reviewing data conversion results is critical to ensure that data from the old system has been accurately and completely migrated to the new system. Accurate data conversion is essential for the integrity and reliability of the accounting system.

NEW QUESTION: 199
Which of the following BEST indicates an effective internal audit quality assurance and improvement program?
A. Oversight of the improvement program by senior management
B. An improved internal audit charter
C. A scope that focuses on high-risk audit engagements
D. Identification of opportunities for continuous improvement
Answer: (SHOW ANSWER)
The goal of a quality assurance and improvement program (QAIP) is to drive continuous enhancement in audit practices and deliver increasing value to stakeholders. Identification and implementation of opportunities for improvement demonstrate that the program is working effectively. Oversight (A) and charter updates (B) are important governance aspects, while

focusing on high-risk audits (C) is a prioritization strategy. However, the hallmark of a successful QAIP is the ability to continuously identify and address gaps, streamline practices, and enhance audit value. ISACA emphasizes agility, adaptability, and ongoing improvement as key success indicators for internal audit functions.

NEW QUESTION: 200

Which of the following information security requirements BEST enables the tracking of organizational data in a bring your own device (BYOD) environment?

A. Employees must use auto-lock features and complex passwords on personal devices.
B. Employees must immediately report lost or stolen mobile devices containing organizational data.
C. Employees must enroll their personal devices in the organization's mobile device management program
D. Employees must sign acknowledgment of the organization's mobile device acceptable use policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 201

Which of the following is the MOST important factor when an organization is developing information security policies and procedures?
A. Consultation with security staff
B. Alignment with an information security framework
C. Compliance with relevant regulations
D. Inclusion of mission and objectives
Answer: (SHOW ANSWER)

NEW QUESTION: 202

Which of the following would BEST assist an IS auditor in understanding the inputs and outputs of a microservice-oriented application?
A. Data flow diagrams
B. Network architecture diagrams
C. Business requirements documentation
D. Entity-relationship diagrams
Answer: (SHOW ANSWER)
Data flow diagrams best assist an IS auditor in understanding how data enters, moves through, and exits a microservice-oriented application, clearly depicting inputs, processing, and outputs across services.

NEW QUESTION: 203

Which of the following should be of MOST concern to an IS auditor reviewing an organization's business impact analysis (BIA)?

A. The BIA was not signed off by executive management
B. System criticality information was only provided by the IT manager
C. A questionnaire was used to gather information as opposed to in-person interviews
D. A risk assessment was not conducted prior to completing the BIA
Answer: (SHOW ANSWER)
The most concerning issue when reviewing an organization's business impact analysis (BIA) is that a risk assessment was not conducted prior to completing the BIA. A risk assessment is essential to identify potential threats and vulnerabilities to the organization's critical systems, which helps inform the BIA by assessing the potential impact of disruptions. Without this assessment, the BIA may lack an adequate understanding of the actual risks faced by the organization, leading to incomplete or ineffective disaster recovery and business continuity planning.

NEW QUESTION: 204
Which of the following is MOST important for an IS auditor to review prior to the migration of acquired software into production?
A. User acceptance test (UAT) report
B. Vendor testing report
C. Expected return on investment (ROI)
D. Source code escrow agreement
Answer: (SHOW ANSWER)
The UAT report provides evidence that the software has been tested by end users to ensure it meets business requirements and functions as expected in a production-like environment. Verifying that UAT was completed successfully is critical to ensuring the software is ready for deployment and will not disrupt business operations.
While the vendor testing report, ROI, and source code escrow agreement are important in their respective contexts, the UAT report directly confirms that the software meets the organization's functional and operational requirements, making it the most critical document to review before migration into production.

NEW QUESTION: 205
Which of the following is MOST important for an IS auditor to validate when reviewing the controls for an organization's quality management system (QMS)?
A. Whether root cause analysis is performed on all failed and rejected changes
B. Whether critical services are delivered in a timely and sustainable manner
C. Whether there is a process to monitor continuous improvement areas and necessary targets
D. Whether the organization follows an industry-recognized service management framework
Answer: (SHOW ANSWER)
A core principle of a quality management system is the focus on continuous improvement. Ensuring that the organization has a process in place to monitor areas for improvement and set necessary targets is critical to maintaining and enhancing the quality of services or products. This

aligns with the fundamental goals of QMS frameworks such as ISO 9001, which emphasize continual improvement and meeting customer expectations.
While the other options are important elements of a quality management approach, validating the process for continuous improvement is essential for the long-term effectiveness and sustainability of the QMS.

NEW QUESTION: 206
Which of the following MOST significantly limits a hacker's ability to use brute force attacks to compromise an encryption scheme?
A. Mathematical algorithms
B. Encryption keys
C. Statistical properties
D. Randomness of key generation
Answer: (SHOW ANSWER)
The randomness of key generation is the most significant factor limiting the success of brute force attacks. Truly random and unpredictable keys make it computationally infeasible for attackers to guess or systematically try all possible key combinations, thereby strengthening the overall encryption scheme.

NEW QUESTION: 207
Which of the following provides the BEST evidence of an organization's disaster recovery readiness?
A. Implementation of action items from the last disaster recovery test
B. Shortened recovery time objectives (RTOs)
C. Senior management sign off of the disaster recovery plan (DRP)
D. Readily available backups over high-speed networks
Answer: (SHOW ANSWER)
The best evidence of an organization's disaster recovery readiness is the implementation of action items from the last disaster recovery test. This demonstrates that the organization has taken corrective actions from previous tests, addressing identified weaknesses, and improving its ability to recover from a disaster. It indicates that the organization is actively refining its disaster recovery processes to ensure they are effective when needed.

NEW QUESTION: 208
A review of an organization's enterprise architecture (EA) BEST enables an IS auditor to determine:
A. alignment of IT service levels with business objectives
B. the organization's level of compliance with regulations
C. adherence to budget for current IT initiative implementations
D. alignment of the IT strategy with business strategy
Answer: (SHOW ANSWER)

Enterprise architecture provides a comprehensive blueprint of how business processes, information flows, applications, and technology infrastructure fit together. By reviewing the EA, an auditor can assess whether IT investments and strategic direction support and enable the organization's business goals, ensuring that IT strategy is aligned with business strategy.

NEW QUESTION: 209
Management has learned the implementation of a new IT system will not be completed on time and has requested an audit. Which of the following audit findings should be of GREATEST concern?
A. Tasks defined on the critical path do not have resources allocated.
B. Milestones have not been defined for all project products.
C. The project manager lacks formal certification.
D. The actual start times of some activities were later than originally scheduled.
Answer: (SHOW ANSWER)

NEW QUESTION: 210
Data from a system of sensors located outside of a network is received by the open ports on a server. Which of the following is the BEST way to ensure the integrity of the data being collected from the sensor system?

A. Implement network address translation on the sensor system.
B. Hash the data that is transmitted from the sensor system.
C. Route the traffic from the sensor system through a proxy server.
D. Transmit the sensor data via a virtual private network (VPN) to the server.
Answer: (SHOW ANSWER)

NEW QUESTION: 211
Which of the following BEST describes a digital signature?
A. It dynamically validates modifications of data.
B. It is under control of the receiver.
C. It is unique to the sender using it.
D. It is capable of authorization.
Answer: (SHOW ANSWER)

NEW QUESTION: 212
Which of the following is the MOST important reason for an IS auditor to conduct a risk assessment when developing a risk-based audit strategy?
A. To ensure high-risk audit areas are identified
B. To ensure proper risk mitigation plans are established
C. To ensure audit risk is defined as a key audit area
D. To ensure audit detection risks are minimized
Answer: (SHOW ANSWER)
The main purpose of conducting a risk assessment when developing a risk-based audit strategy is to identify and prioritize areas with the highest risk to the organization. This allows the IS auditor to allocate audit resources effectively and focus on areas that have the greatest potential impact on achieving organizational objectives.

NEW QUESTION: 213
Which of the following risk scenarios is BEST mitigated through the use of a data loss prevention (DLP) tool?
A. An employee is sending company documents to an external email to increase productivity
B. A former employee retains access to an application that authenticates via single sign-on (SSO)
C. An employee uses production data in a test environment
D. An employee selects the incorrect data classification on documents
Answer: (SHOW ANSWER)
A Data Loss Prevention (DLP) tool is designed to monitor, detect, and prevent unauthorized sharing or transfer of sensitive data outside the organization. It is best suited to mitigate scenarios where employees may intentionally or unintentionally send company documents to external email addresses, which poses a risk of data leakage.

NEW QUESTION: 214
In which data loss prevention (DLP) deployment model is data inspection and policy enforcement performed at the organization's perimeter or gateway?
A. Hybrid DLP
B. Cloud-based DLP
C. Endpoint-based DLP
D. Network-based DLP
Answer: (SHOW ANSWER)
Network-based DLP solutions inspect data in motion at an organization's network perimeter or gateway, applying policies to traffic before it leaves or enters the network. This placement enables real-time monitoring and blocking of sensitive information transfers at the gateway.

NEW QUESTION: 215
Which of the following could invalidate the digital evidence collected in a forensic investigation?
A. Law enforcement was not involved in evidence collection

B. Analysis was not done on the original media
C. The evidence was handled by more than one person
D. A write blocker was not used when evidence was collected
Answer: (SHOW ANSWER)
The use of a write blocker is crucial in forensic investigations to ensure that digital evidence is not altered during the collection process. If a write blocker was not used, it could result in the modification of the original data, potentially invalidating the evidence and compromising the integrity of the forensic investigation.

NEW QUESTION: 216
A company requires that all program change requests (PCRs) be approved and all modifications be automatically logged. Which of the following is audit procedures will BEST determine whether unauthorized changes have been made to production programs?
A. Use source code comparison software to determine whether any changes have been made to a sample of programs since the last audit date.
B. Trace a sample of complete PCR forms to the log of all program changes.
C. Trace a sample of program changes from the log to completed PCR forms.
D. Review a sample of PCRs for proper approval throughout the program change process.
Answer: (SHOW ANSWER)

NEW QUESTION: 217
Which of the following is the PRIMARY benefit of leveraging an IT-related framework when conducting an audit?
A. It provides a comprehensive list of potential audit findings.
B. It provides a standardized model for the audit subject.
C. It ensures alignment with audit standards.
D. It supports the credibility of the audit report.
Answer: (SHOW ANSWER)
Using an established IT-related framework (such as COBIT or ISO/IEC 27001) gives the IS auditor a structured and standardized model to assess controls, processes, and governance. This ensures consistent evaluation criteria and improves the reliability and comparability of audit results.

NEW QUESTION: 218
Which of the following BEST facilitates the successful implementation of IT performance monitoring?
A. Adopting global standards and measurement norms
B. Determining goals for IT resources and processes
C. Identifying tools to automate performance measurement
D. Establishing templates for periodic reporting to management
Answer: (SHOW ANSWER)

The best way to facilitate the successful implementation of IT performance monitoring is by determining goals for IT resources and processes. Clear, measurable goals help align monitoring efforts with the organization's strategic objectives, enabling the identification of key performance indicators (KPIs) and ensuring that performance is effectively tracked and evaluated against established benchmarks.

NEW QUESTION: 219
Which of the following job scheduling schemes for operating system is MOST likely to adequately balance protection of workstations with user requirements?
A. Automated patching jobs followed by a scheduled restart outside of business hours
B. End users can initiate patching including subsequent system restarts
C. Automated patching and immediate restart
D. Applying only those patches not requiring a system restart
Answer: (SHOW ANSWER)
This approach ensures that critical patches are applied promptly while minimizing disruption to users by scheduling restarts outside of business hours. It balances the need for system protection through timely patching with the requirement to maintain productivity during working hours.

NEW QUESTION: 220
During audit planning for the review of an Internet of Things (IoT) implementation program, an IS auditor requests the organization's information risk policy. Which of the following pieces of information would the auditor PRIMARILY expect to find in the policy?

A. The risk register for associated risks
B. A detailed inventory of vulnerabilities
C. The defined risk appetite for new technologies
D. Guidelines on implementing security controls
Answer: (SHOW ANSWER)
An information risk policy primarily defines the organization's overall approach to managing risk, including its risk appetite and tolerance levels - especially for emerging technologies like IoT. This helps guide decision-making and control implementation consistent with the organization's accepted level of risk.

NEW QUESTION: 221
Which of the following is MOST useful to an IS auditor performing a review of access controls for a document management system?
A. Information provided by the audit team lead on the authentication systems used by the department
B. Policies and procedures for managing documents provided by department heads
C. Previous audit reports related to other departments' use of the same system
D. A system-generated list of staff and their project assignments, roles, and responsibilities
Answer: (SHOW ANSWER)

https://www.securends.com/blog/best-ways-to-conduct-user-access-reviews/

NEW QUESTION: 222
Which of the following controls BEST helps to prevent sensitive data leakage when using APIs?
A. Maintaining an updated inventory of all APIs used in the organization
B. Implementing strong passwords to authenticate users
C. Conducting periodic scans of all APIs to identify vulnerabilities
D. Ensuring APIs authenticate endpoints before allowing access
Answer: (SHOW ANSWER)
Endpoint authentication ensures that only authorized systems or users can access the API, preventing unauthorized data exposure and reducing the risk of sensitive data leakage. This control enforces secure communication and trust between interacting systems.

NEW QUESTION: 223
Which of the following should an IS auditor recommend be done FIRST when an organization is planning to implement an IT compliance program?
A. Analyze historical compliance-related audit findings
B. Identify applicable laws, regulations, and standards
C. Research and purchase an industry-recognized IT compliance tool
D. Identify staff training needs related to compliance requirements
Answer: (SHOW ANSWER)
This is the foundation for any compliance program, as it ensures that the organization is aware of the legal and regulatory requirements it must adhere to. Once the relevant laws, regulations, and standards are identified, the organization can then proceed with further steps, such as addressing past audit findings, selecting tools, or providing staff training to meet those compliance requirements.
Without understanding the applicable requirements, any further efforts may be misaligned or ineffective.

NEW QUESTION: 224
A staff accountant regularly uploads spreadsheets with inventory levels to the organization's financial reporting system. The transfers are executed through a customized interface created by an in-house developer. Which of the following is MOST important for the IS auditor to confirm during a review of the interface?
A. The data in the spreadsheet is correctly recorded in the financial system.
B. The financial system transfers are performed by the accountant at predefined intervals.
C. The spreadsheets do not contain malware or malicious macros.
D. The data transfer connection does not support full duplex communication.
Answer: A (LEAVE A REPLY)
The primary audit concern is data integrity-ensuring that the data uploaded via the custom interface is accurately and completely transferred to the financial system.

Option A directly addresses data accuracy and integrity.
Option B (timing) is secondary compared to correctness.
Option C (malware checks) is important but handled by security controls, not the primary audit concern here.
Option D (duplex communication) is irrelevant to ensuring accurate financial records.

NEW QUESTION: 225
An IS auditor discovers there are no documented security procedures. What should be the NEXT step?
A. Identify and evaluate the current security practices implemented by the organization.
B. Identify compensating controls for the lack of documentation.
C. Assist information security management with preparing security procedures.
D. Review security incident logs and related metrics.
Answer: (SHOW ANSWER)
When no documented security procedures exist, the IS auditor's next step is to identify and assess the security practices currently in place. This allows the auditor to determine whether effective controls are operating, even if undocumented, and to evaluate the associated risks before recommending formal documentation.

NEW QUESTION: 226
Which of the following should be an IS auditor's PRIMARY focus when auditing a file-sharing system used for collaboration among remote teams?
A. Evaluating the encryption and access control mechanisms of the file-sharing system
B. Ensuring communications and records are stored according to the organization's data retention policy
C. Reviewing the integration of the file-sharing system with external communication tools
D. Assessing the bandwidth consumption of the file-sharing system
Answer: A (LEAVE A REPLY)
The primary concern for an IS auditor is whether the file-sharing system adequately protects sensitive information. Strong encryption and effective access controls are critical to prevent unauthorized access and data leakage, especially in a remote collaboration environment.

NEW QUESTION: 227

An organization has recently implemented additional application programming interfaces (APIs) to enhance data exchange with vendors. Which of the following is MOST important to ensure coverage of API-related risks during the next API management process audit?
A. Evaluating the compliance of APIs with the organization's standards and best practices
B. Verifying the adequacy of disaster recovery and business continuity plans for critical APIs
C. Testing the authorization mechanisms in place to secure API endpoints
D. Reviewing the process of API documentation and version control to ensure accuracy and consistency
Answer: C (LEAVE A REPLY)
Authorization controls are critical in API security because they ensure that only authenticated and properly authorized users or systems can access specific data or functions. Weak or missing authorization can lead to data breaches or unauthorized data manipulation, making this the most important focus area for an API management process audit.

NEW QUESTION: 228
When conducting an audit of an organization's use of AI in its customer service chatbots, an IS auditor should PRIMARILY focus on the:
A. AI system's compliance with industry security standards
B. safeguarding of personal data processing by the AI system
C. speed and accuracy of chatbot responses to customer queries
D. AI system's ability to handle multiple customer queries at once
Answer: (SHOW ANSWER)
The foremost concern when auditing AI chatbots in customer service is ensuring that personal and sensitive customer data are handled in compliance with privacy regulations and organizational policies. Verifying appropriate data anonymization, access controls, and consent management directly addresses the risk of unauthorized disclosure or misuse of customer information, which is paramount in maintaining trust and regulatory compliance. Performance metrics (speed, concurrency, accuracy) and security standards are important but secondary to ensuring personal data protection.

NEW QUESTION: 229
An IS auditor is planning a review of an organization's robotic process automation (RPA) technology. Which of the following MUST be included in the audit work plan?
A. Integration architecture
B. Change management
C. Cost-benefit analysis
D. Employee training content
Answer: (SHOW ANSWER)
Change management is a critical component of any audit involving robotic process automation (RPA) technology. Since RPA systems are designed to automate processes, any changes made to the bots or workflows need to be properly managed to ensure they are aligned with business

objectives and do not introduce new risks. A review of change management ensures that RPA deployments and modifications are documented, tested, and approved in a controlled manner, which helps maintain system integrity and reduces the risk of errors.

NEW QUESTION: 230

Which of the following would be MOST useful to an IS auditor when making recommendations to enable continual improvement of IT processes over time?

A. IT incident log
B. IT risk register
C. Maturity model
D. Benchmarking studies
Answer: (SHOW ANSWER)
https://www.viima.com/blog/continuous-improvement-tools

NEW QUESTION: 231
Which of the following is the BEST method to safeguard data on an organization's laptop computers?
A. Disabled USB ports
B. Full disk encryption
C. Multi-factor authentication (MFA)
D. Passkey phrases
Answer: (SHOW ANSWER)
The greatest risk to laptop computers is data exposure in case of theft or loss. The most effective safeguard is full disk encryption, which ensures that even if the device is stolen, data remains unreadable without the encryption key.
Disabled USB ports (A): Prevents some forms of data exfiltration but does not protect stored data.
MFA (C): Protects user authentication but not the data if the disk is removed.
Passkey phrases (D): Improves authentication strength but is weaker than encryption for data protection.

NEW QUESTION: 232
Which of the following issues identified during a formal review of an organization's information security policies presents the GREATEST potential risk to the organization?
A. The policies are not aligned with the information security risk appetite.
B. The policies are not available to key risk stakeholders.
C. The policies are not based on industry best practices for information security.
D. The policies have not been reviewed by the risk management committee.
Answer: (SHOW ANSWER)

NEW QUESTION: 233

Which of the following is the MOST cost-effective way to determine the effectiveness of a business continuity plan (BCP)?

A. Stress test

B. Tabletop exercise

C. Full operational test

D. Post-implementation review

Answer: (SHOW ANSWER)

A tabletop exercise is the most cost-effective method to test the BCP because it simulates scenarios and walks through responses without disrupting operations.

Stress test (A): More resource-intensive and may disrupt services.

Full operational test (C): Provides the highest assurance but is costly and disruptive.

Post-implementation review (D): Evaluates after actual incidents, not proactive.

NEW QUESTION: 234

An organization has moved all of its infrastructure to the cloud. Which of the following would be an IS auditor's GREATEST concern related to the organization's ability to continue operations in case of a disaster?

A. There is no evidence that disaster recovery plan (DRP) testing was performed after the migration

B. Only business-critical servers were configured with redundancy services on the cloud service provider

C. The step-by-step recovery process was not updated in the disaster recovery plan (DRP) after the migration

D. The previous infrastructure was not retained to support business operations in case of a disaster

Answer: (SHOW ANSWER)

The greatest concern would be that the step-by-step recovery process was not updated in the disaster recovery plan (DRP) after the migration. A DRP that is not updated to reflect changes in infrastructure, such as moving to the cloud, would leave the organization unprepared to recover from a disaster. The recovery procedures need to be aligned with the new cloud-based infrastructure to ensure continuity of operations.

NEW QUESTION: 235

Which of the following would be of GREATEST concern when testing an organization's controls around social engineering threats?

A. Incident handling procedures are not included in security awareness sessions

B. Staff are not aware of information asset classifications

C. Biometric authentication is not utilized

D. The intrusion detection system (IDS) is not configured properly

Answer: (SHOW ANSWER)

The greatest concern is the absence of incident handling procedures in security awareness sessions. Without proper training on how to recognize and respond to social engineering attempts, staff may fail to take appropriate actions when such threats occur. This can lead to greater vulnerability and an ineffective response to potential breaches, undermining the organization's overall security posture.

NEW QUESTION: 236
Which of the following should be the PRIMARY concern for the IT department head when implementing operational log management?
A. Diversity of log formats generated by different IT resources
B. Retention and storage issues due to log volume
C. Resistance by operational users
D. Impact on performance of IT resources
Answer: D (LEAVE A REPLY)
While all the other concerns (log format diversity, storage issues, and user resistance) are important, the impact on the performance of IT resources is critical because operational log management can potentially degrade system performance if not handled properly. Log collection, processing, and storage can consume significant system resources, such as CPU, memory, and storage space, which may affect the availability and efficiency of IT systems. Ensuring that log management does not negatively impact the performance of critical IT services should be the primary focus.
Once performance considerations are addressed, other factors like storage, format diversity, and user resistance can be managed effectively.

NEW QUESTION: 237
Which of the following documents would be MOST useful in detecting a weakness in segregation of duties?
A. Data flow diagram
B. Process flowchart
C. Entity-relationship diagram
D. Systems flowchart
Answer: (SHOW ANSWER)

NEW QUESTION: 238
An IS auditor decides to review a data inventory list captured directly from a system instead of relying on an interview with the system owner. Which of the following provides the BEST justification for the auditor's decision?
A. Independence of the evidence provider
B. Qualification of the evidence provider
C. Reliability of the evidence
D. Timing of the evidence

Answer: (SHOW ANSWER)
System-generated data is generally more reliable than interview evidence, which is subjective and prone to bias. Audit standards emphasize evidence that is sufficient and appropriate, where appropriateness relates to relevance and reliability.

NEW QUESTION: 239
Which of the following is the MOST important reason to implement version control for an end-user computing (EUC) application?
A. To ensure that older versions are available for reference
B. To ensure compatibility between different versions of the application
C. To ensure that only authorized users can access the application
D. To ensure that only the latest approved version of the application is used
Answer: (SHOW ANSWER)

NEW QUESTION: 240
Which of the following is the PRIMARY function of an internal IS auditor when the organization acquires a new IT system to support its business strategy?

A. Identifying significant IT errors and fraud
B. Assessing system development life cycle (SDLC) controls
C. Implementing risk and control gap mitigation
D. Evaluating IT risk and controls
Answer: (SHOW ANSWER)
The internal IS auditor's foremost responsibility during a system acquisition is to assess whether IT risks are identified and that appropriate control measures are in place to manage those risks. This evaluation ensures the new system supports the business strategy within a controlled risk framework.

NEW QUESTION: 241
When protecting the confidentiality of information assets, the MOST effective control practice is the:
A. utilization of a dual-factor authentication mechanism.
B. configuration of read-only access to all users.
C. awareness training of personnel on regulatory requirements.
D. enforcement of a need-to-know access control philosophy.
Answer: (SHOW ANSWER)

NEW QUESTION: 242
An IS auditor found that operations personnel failed to run a script contributing to year-end financial statements. Which of the following is the BEST recommendation?
A. Retrain operations personnel.
B. Bring staff with financial experience into operations.
C. Update the operations manual.
D. Implement a closing checklist.
Answer: (SHOW ANSWER)

NEW QUESTION: 243
Which of the following is MOST important to ensure successful implementation when an organization decides to purchase software from available products on the market?
A. Requirements definition
B. Post-implementation review
C. Support and maintenance contract
D. Software escrow
Answer: (SHOW ANSWER)
Defining clear, comprehensive, and testable requirements is critical before selecting and implementing a software product. Without well-documented requirements, the risk of choosing a solution that does not align with business needs increases significantly. A support contract (C) is important for long-term use, and escrow (D) may protect against vendor insolvency, but neither ensures that the product fits the organization's objectives. A post-implementation review (B) only evaluates success after implementation, which may be too late to correct fundamental misalignment. ISACA's COBIT framework (BAI03 and BAI05) stresses the importance of requirements gathering as the foundation for effective solution acquisition and development.

NEW QUESTION: 244
Which of the following is the PRIMARY purpose of conducting a control self-assessment (CSA)?
A. To replace audit responsibilities
B. To reduce control costs
C. To promote control ownership
D. To enable early detection of risks
Answer: (SHOW ANSWER)
The main goal of a CSA is to involve business units and process owners in assessing the effectiveness of internal controls and managing risks. By doing so, it encourages greater accountability and ownership of controls within the organization, ensuring that those who are closest to the processes are actively involved in maintaining and improving the control environment.

While early detection of risks, potential cost reduction, and other benefits can result from a CSA, the central purpose is to foster control ownership among the business units and process owners.

NEW QUESTION: 245
Which of the following approaches would present the GREATEST concern for the implementation of a quality assurance (QA) function?
A. Developers introducing the changes will review the work, as they are most familiar with them
B. Peer developers from the same development team who unfamiliar with the changes will review them
C. Developers from a separate development team in the organization will review the submitted changes
D. Reviewers outside the development group who do not have development roles with review the changes
Answer: (SHOW ANSWER)
The greatest concern with this approach is that developers who introduced the changes reviewing their own work can lead to biases and a lack of objectivity. They may overlook defects or issues, either unintentionally or due to familiarity with the code. Independent reviews, preferably from peers or teams who did not introduce the changes, are more effective in identifying potential issues.

NEW QUESTION: 246
Following a discussion on the results of a recent audit engagement, the process owner of the audited area has provided an action plan addressing the gaps and recommendations. The auditor disagrees with some of the responses where the process owner is accepting a level of residual risk that is not within the organization's risk appetite. What is the auditor's BEST course of action?
A. Include the issue in the next report to the audit committee.
B. Inform executive management of the residual risk.
C. Accept the action plan proposed by the process owner.
D. Escalate the situation to audit management.
Answer: (SHOW ANSWER)
When an auditor finds that the process owner is accepting residual risk beyond the organization's defined risk appetite, it is not appropriate to accept the action plan or wait until the next committee report.
Escalating to audit management (D) is the correct step. Audit management can then determine whether to escalate further to executive management or the audit committee.
Including in the next report (A) delays timely risk response.
Informing executive management directly (B) bypasses the audit reporting hierarchy.
Accepting the plan (C) would be inappropriate as it ignores risk governance.

NEW QUESTION: 247

Which of the following is the MOST important task of an IS auditor during an application post-implementation review?

A. Conduct a business impact analysis (BIA)

B. Perform penetration testing

C. Identify project delays

D. Verify user access controls

Answer: (SHOW ANSWER)

Ensuring that appropriate user access controls are in place is crucial to protecting the application's data and functionality from unauthorized access or misuse. This task directly impacts the security and integrity of the application post-implementation. Access controls help ensure that only authorized users can access sensitive data and perform critical functions, which is a key focus area for an IS auditor.

While a business impact analysis (BIA), penetration testing, and identifying project delays are important activities, they may not be as critical in the immediate post-implementation review as verifying that proper user access controls have been implemented. This is essential for maintaining security and ensuring that the system operates as intended in a secure environment.

NEW QUESTION: 248

Reviewing which of the following would provide the BEST indication that a project is progressing as planned?

A. Traceability matrix

B. Earned value analysis (EVA) results

C. Identification of the critical path

D. Work breakdown structure

Answer: (SHOW ANSWER)

Earned value analysis (EVA) integrates project scope, schedule, and cost to measure project performance objectively. It provides a clear indication of whether the project is on track regarding both progress and budget, making it the best indicator that a project is progressing as planned.

NEW QUESTION: 249

In planning a major system development project, function point analysis would assist in:

A. estimating the elapsed time of the project

B. analyzing the functions undertaken by system users as an aid to job redesign

C. determining the business functions undertaken by a system or program

D. estimating the size of a system development task

Answer: (SHOW ANSWER)

Function point analysis is primarily used to estimate the size of a system development task. It helps assess the complexity of the system by measuring the functionality provided to the user, which can then be used to estimate development effort, time, and resources required for the project.

NEW QUESTION: 250

The operations team of an organization has reported an IS security attack. Which of the following should be the FIRST step for the security incident response team?

A. Perform a damage assessment.

B. Document lessons learned.

C. Prioritize resources for corrective action.

D. Report results to management.

Answer: (SHOW ANSWER)

NEW QUESTION: 251

Which of the following is the MOST significant risk related to shadow IT?

A. Inappropriate utilization may hinder IT's ability to provide support

B. Use a shadow IT over time may cause production slowdowns

C. Software or hardware may be unnecessarily duplicated

D. Necessary controls may not be in place

Answer: (SHOW ANSWER)

The most significant risk related to shadow IT is the lack of necessary controls, as the use of unauthorized IT resources can bypass security measures, compliance policies, and data protection controls, potentially leading to vulnerabilities and increased exposure to risks.

NEW QUESTION: 252

An IS auditor is reviewing an origination's release management practices and observes inconsistent and inaccurate estimation of the size and complexity of business application development projects. Which of the following should the auditor recommend to address this issue?

A. Agile development approach

B. Rapid application development

C. Function point analysis

D. Critical path methodology

Answer: (SHOW ANSWER)

NEW QUESTION: 253

Which of the following is MOST important to consider when assessing the scope of privacy concerns for an IT project?

A. Applicable laws and regulations

B. Data ownership

C. Business requirements and data flows

D. End user access rights

Answer: (SHOW ANSWER)

NEW QUESTION: 254

An IS auditor observes that an organization's systems are being used for cryptocurrency mining on a regular basis. Which of the following is the auditor's FIRST course of action?
A. Report the incident immediately
B. Recommend changing the organization's firewall settings
C. Consult the organization's acceptable use policy
D. Require mining software to be uninstalled
Answer: (SHOW ANSWER)
The auditor's first course of action should be to consult the organization's acceptable use policy (AUP) to determine whether cryptocurrency mining is permitted or violates organizational rules. This establishes a clear understanding of the organization's stance on the activity and informs the appropriate next steps. Without reviewing the policy, it is premature to report the incident or recommend changes.

NEW QUESTION: 255
Which of the following is MOST important to consider when developing a service level agreement (SLA)?
A. Description of the services from the viewpoint of the client organization
B. Detailed identification of work to be completed
C. Provisions for regulatory requirements that impact the end users' businesses
D. Description of the services from the viewpoint of the provider
Answer: (SHOW ANSWER)
An SLA should primarily define services from the client organization's viewpoint to ensure expectations, performance measures, and service outcomes are clearly aligned with business needs and user requirements.

NEW QUESTION: 256
What is the BEST control to address SQL injection vulnerabilities?
A. Secure Sockets Layer (SSL) encryption
B. Digital signatures
C. Unicode translation
D. Input validation
Answer: (SHOW ANSWER)

NEW QUESTION: 257
Which of the following is the MOST important consideration for an IS auditor when assessing the adequacy of an organizations information security policy?
A. Business objectives
B. Compliance with industry best practice
C. IT steering committee minutes
D. Alignment with the IT tactical plan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 258
Which of the following would BEST assist an IS auditor in understanding the inputs and outputs of a microservice-oriented application?
A. Data flow diagrams
B. Network architecture diagrams
C. Business requirements documentation
D. Entity-relationship diagrams
Answer: (SHOW ANSWER)
For a microservices architecture, the most effective way to understand data movement between components is through data flow diagrams (DFDs). DFDs clearly show inputs, outputs, processes, and data stores, helping auditors trace data movement across distributed services.
Option A: Correct - DFDs highlight application inputs/outputs.
Option B: Network diagrams show infrastructure but not logical data flows.
Option C: Business requirements document functional needs, not technical flows.
Option D: ER diagrams describe database structures, not process flows.

NEW QUESTION: 259
The IS quality assurance (QA) group is responsible for:
A. monitoring the execution of computer processing tasks.
B. ensuring that the output received from system processing is complete.
C. designing procedures to protect data against accidental disclosure.
D. ensuring that program changes adhere to established standards.
Answer: (SHOW ANSWER)

NEW QUESTION: 260
Which of the following is the PRIMARY benefit of enabling database audit trails?
A. Accountability can be determined.
B. Transactions can be researched.
C. Separation of duties can be confirmed.
D. Availability can be improved.
Answer: (SHOW ANSWER)

The primary benefit of enabling database audit trails is to establish accountability by tracking who performed specific actions, when they occurred, and what changes were made. This ensures user activities can be traced, supporting security monitoring, compliance, and forensic analysis.

NEW QUESTION: 261
When conducting a post-implementation review, which of the following is the BEST way to determine whether the value from an IT project has been achieved?
A. Conduct peer benchmarking exercises
B. Calculate the return on investment (ROI)
C. Assess impact on the IT portfolio
D. Survey end users
Answer: (SHOW ANSWER)
ROI directly measures the financial benefits realized versus the costs incurred, providing an objective quantification of whether the project delivered the expected value.

NEW QUESTION: 262
Which of the following features would BEST address risk associated with data at rest when evaluating a data loss prevention (DLP) solution?
A. Printing of scan files
B. File movement detection
C. Enforcement of access policies
D. Storage-scanning technology
Answer: (SHOW ANSWER)
Storage-scanning technology enables DLP solutions to scan data at rest across different storage locations (e.g., databases, file systems, or cloud storage) to identify and protect sensitive information. This helps ensure that sensitive data is properly secured and that any unauthorized storage or access can be flagged and mitigated. It directly addresses the risk associated with storing sensitive data in unauthorized or unsecured locations.
While file movement detection, access policies, and printing controls are important, storage-scanning technology specifically focuses on discovering and securing data at rest, which is the primary concern for managing the risk of static data exposure.

NEW QUESTION: 263
Which of the following is the PRIMARY objective of implementing privacy-related controls within an organization?
A. To comply with legal and regulatory requirements
B. To provide options to individuals regarding use of their data
C. To identify data at rest and data in transit for encryption
D. To prevent confidential data loss
Answer: (SHOW ANSWER)

NEW QUESTION: 264
Which of the following is the MOST important regulatory consideration for an organization determining whether to use its customer data to train AI algorithms?
A. Collection of data and obtaining data subject consent
B. Ethical and optimal utilization of data computing resources
C. Documentation of AI algorithm accuracy during the training process
D. Continuous monitoring of AI algorithm performance
Answer: (SHOW ANSWER)
The most important regulatory consideration when using customer data to train AI algorithms is ensuring that data is collected lawfully and that explicit consent from data subjects has been obtained where required. This aligns with data protection laws such as GDPR, which emphasize lawful processing and informed consent for personal data use.

NEW QUESTION: 265
An IS auditor performed tests to evaluate the readiness of developed software for implementation. Which of the following test results BEST indicates that the software meets security requirements?
A. The software processes only required data types.
B. The passwords meet both complexity and aging criteria.
C. Users can only perform tasks and functions assigned to their roles.
D. Users are required to utilize encrypted connections.
Answer: (SHOW ANSWER)
Ensuring users can only perform tasks and functions assigned to their roles demonstrates effective logical access controls and enforcement of the principle of least privilege, which is a core indicator that security requirements have been properly implemented in the software.

NEW QUESTION: 266
Which of the following controls would BEST protect against internet sniffers conducting a replay attack?
A. Packet-filtering router
B. Digital signature
C. Properly configured firewall
D. Time-stamped data encryption
Answer: (SHOW ANSWER)
Time-stamped data encryption helps prevent replay attacks by ensuring that each transmission is unique and valid only within a specific timeframe. Even if intercepted, the encrypted data cannot be reused by an attacker because the timestamp invalidates old or duplicated messages.

NEW QUESTION: 267
Which of the following would be of concern to an IS auditor reviewing development practices for sensitive proprietary code?

A. Developer workstations do not have internet access.
B. Developer performance is not measured based on lines of code written.
C. Developers are debugging by uploading the code into a publicly available generative AI tool.
D. Developers are not using generative AI tools to maximize efficiency.
Answer: (SHOW ANSWER)
Uploading sensitive proprietary code into a publicly available generative AI tool creates a significant risk of unauthorized disclosure, loss of intellectual property, and potential reuse of the code outside the organization's control, directly compromising confidentiality and competitive advantage.

NEW QUESTION: 268
A zero-day vulnerability with a critical severity score has been published for a core business application. Which of the following should be done FIRST to address this vulnerability?
A. Identify the version of software the organization is using
B. Initiate the organization's incident response plan
C. Work with the vendor to deploy patches in the production environment
D. Propose risk acceptance until a patch is deployed
Answer: (SHOW ANSWER)
The first step to address a zero-day vulnerability is to identify the version of the software the organization is using. This ensures that the vulnerability is applicable to the specific version in use and helps in determining the appropriate remediation steps, such as finding available patches or mitigating controls. Once the version is identified, the organization can proceed with patch deployment, risk assessment, or incident response as needed.

NEW QUESTION: 269
Which of the following is an IS auditor's MOST important step in a privacy audit?
A. Assess the controls in place for data management.
B. Determine whether privacy training is being conducted for employees.
C. Review third-party agreements for adequate personally identifiable information (PII) protection measures.
D. Analyze all stages of the personally identifiable information (PII) data life cycle to identify potential risks.
Answer: (SHOW ANSWER)
The most important step in a privacy audit is to ensure that all risks associated with PII handling are identified. This requires analyzing the entire PII data life cycle--from collection, processing, storage, and transfer to retention and destruction.
Option A: Reviewing data management controls is part of the audit but is narrower than life cycle coverage.
Option B: Privacy training is necessary, but training alone doesn't ensure compliance.
Option C: Reviewing third-party agreements is important but only covers outsourced risks.
Option D: Provides comprehensive coverage of privacy risks across all stages.

NEW QUESTION: 270

If not properly secured, which of the following could result in the hijacking of HTTP traffic during a transaction between a user and a web application, allowing an attacker to impersonate the victim?

A. Session ID

B. Device ID

C. Server ID

D. Application ID

Answer: (SHOW ANSWER)

A session ID uniquely identifies a user's active session with a web application. If it is not properly secured - such as through encryption or secure cookies - an attacker can intercept and hijack the session, impersonating the user and gaining unauthorized access to the application.

NEW QUESTION: 271

IT management wants transferred staff to have current and previous role access to facilitate transitioning and training of new staff. Which of the following is the GREATEST risk to the organization from this practice?

A. An increased likelihood that internal fraud will not be detected

B. An increased impact from loss of key staff

C. An increased number of help desk tickets due to password changes

D. An increased number of user access recertification records

Answer: (SHOW ANSWER)

Allowing transferred staff to retain access from previous roles violates the principle of least privilege and increases the risk of inappropriate access. This creates a greater likelihood that internal fraud or unauthorized activities could occur without detection, as users may retain access to systems or data unrelated to their current responsibilities.

NEW QUESTION: 272

An organization is implementing a data loss prevention (DLP) system in response to a new regulatory requirement. Reviewing which of the following would be MOST helpful in evaluating the system's design?

A. System manuals

B. Enterprise architecture (EA)

C. Historical record of data breaches
D. Industry trends
Answer: (SHOW ANSWER)
https://www.digitalguardian.com/blog/how-evaluate-dlp-solutions-6-steps-follow-and-10-questions-ask

NEW QUESTION: 273
An IS auditor finds that some employees are using public cloud-based AI tools. Which of the following presents the GREATEST concern?
A. Copyright infringements
B. Cost overruns
C. Data leakage
D. Data reliability
Answer: (SHOW ANSWER)
The greatest concern in this scenario is data leakage. Public cloud-based AI tools may not provide sufficient security controls, and sensitive organizational data could be exposed to unauthorized access or misuse. This could lead to serious privacy and compliance risks, especially if the data is not properly encrypted or managed according to security policies.

NEW QUESTION: 274
An IS auditor evaluating a policy should be MOST concerned about the lack of a:
A. distribution list.
B. version history.
C. document owner.
D. creation date.
Answer: (SHOW ANSWER)
The absence of a document owner is the greatest concern because ownership ensures accountability for maintaining, reviewing, and updating the policy. Without a designated owner, the policy may become outdated, inconsistently applied, or lack enforcement.

NEW QUESTION: 275
Which of the following provides the BEST evidence that all elements of a business continuity plan (BCP) are operating effectively?
A. Walk-through test results
B. Full operational test results
C. Simulation test results
D. Tabletop test results
Answer: (SHOW ANSWER)
https://www.sweetprocess.com/business-continuity-plan/

NEW QUESTION: 276

Which of the following should be of GREATEST concern to an IS auditor reviewing controls around an artificial intelligence (AI) system in an organization?
A. Contracted developers have access to the knowledge base for maintenance purposes
B. Development of the knowledge base was outsourced to vendors
C. Basic assumptions and formulas used to develop the decision logic were not documented
D. The policy and procedure guide and its decision logic were reviewed once annually
Answer: (SHOW ANSWER)
The greatest concern for an IS auditor would be the lack of documentation for the basic assumptions and formulas used to develop the AI system's decision logic. This absence can lead to issues with transparency, accountability, and the ability to audit or validate the system's outputs. Proper documentation is critical for ensuring that the system operates as intended and that its decisions can be explained and justified if questioned.

NEW QUESTION: 277
Transaction records from a business database were inadvertently deleted, and system operators decided to restore from a snapshot copy. Which of the following provides the BEST assurance that the transactions were recovered successfully?
A. Recount the transaction records to ensure no records are missing.
B. Rerun the process on a backup machine to verify the results are the same.
C. Compare transaction values against external statements to verify accuracy.
D. Review transaction recovery logs to ensure no errors were recorded.
Answer: (SHOW ANSWER)

NEW QUESTION: 278
Which of the following should be an IS auditor's MOST important consideration when auditing an organization's system capacity management processes?
A. Verifying the frequency and effectiveness of data backup procedures
B. Assessing response times during regular operations and periods of high demand
C. Reviewing the organization's cybersecurity capabilities
D. Evaluating the most recent business impact analysis (BIA)
Answer: (SHOW ANSWER)
System capacity management is primarily concerned with ensuring systems can meet performance requirements under both normal and peak conditions. Assessing response times during regular operations and periods of high demand directly confirms whether capacity planning and monitoring are effective in supporting business needs.

NEW QUESTION: 279
Which of the following should be of GREATEST concern to an IS auditor when auditing an organization's IT strategy development process?
A. The IT strategy was developed before the business plan
B. A business impact analysis (BIA) was not performed to support the IT strategy

C. The IT strategy was developed based on the current IT capability
D. Information security was not included as a key objective in the IT strategic plan
Answer: (SHOW ANSWER)
The IT strategy must align with and support the overall business strategy and objectives. Developing an IT strategy before the business plan means there is a risk that the IT initiatives may not be aligned with the business goals, leading to misallocation of resources and technology investments that do not meet business needs.
While the other issues - lack of a BIA, developing the strategy based on current IT capabilities, and the absence of information security as a key objective - are important, they are secondary to ensuring that the IT strategy is aligned with the business strategy. Without this alignment, the IT strategy may fail to provide value to the organization.

NEW QUESTION: 280
A post-implementation review was conducted by issuing a survey to users. Which of the following should be of GREATEST concern to an IS auditor?

A. The survey form template did not allow additional feedback to be provided.
B. The survey results were not presented in detail to management.
C. The survey questions did not address the scope of the business case.
D. The survey was issued to employees a month after implementation.
Answer: (SHOW ANSWER)
https://www.iaasb.org/_flysystem/azure-private/publications/files/IAASB-Auditor-Reporting-PIR-Survey-final-Main-Document-Update_0.pdf

NEW QUESTION: 281
How does public key infrastructure (PKI) help to verify that a digitally signed document is not a forgery?
A. By decrypting the signature with the signer's public key
B. By verifying the signature with the signer's private key
C. By checking the signature against the receiver's public key
D. By checking the signed document's audit history
Answer: (SHOW ANSWER)
In PKI, when a document is digitally signed:
The signer uses their private key to create the signature.
The recipient uses the signer's public key to decrypt and verify the signature.
If the decrypted hash matches the document's computed hash, the document is authentic and unaltered.
Option A: Correct - verification is done with the public key.
Option B: Incorrect - the private key is only used to sign, not verify.
Option C: Wrong - the receiver's public key is irrelevant.
Option D: Not applicable - audit history is not part of PKI validation.

NEW QUESTION: 282
Which of the following system attack methods is executed by entering malicious code into the search box of a vulnerable website, causing the server to reveal restricted information?
A. Man-in-the-middle
B. Denial of service (DoS)
C. SQL injection
D. Cross-site scripting
Answer: (SHOW ANSWER)
https://www.crowdstrike.com/cybersecurity-101/malicious-code/

NEW QUESTION: 283
During the forensic investigation of a cyberattack involving credit card data, which of the following is MOST important to ensure?
A. All staff in the payment card unit are interviewed
B. Adequate card security features are activated
C. Proper chain of custody is maintained
D. The company's payment platforms are blocked
Answer: (SHOW ANSWER)
The most important factor during the forensic investigation of a cyberattack involving credit card data is maintaining proper chain of custody. This ensures that the integrity of evidence is preserved and that it remains admissible in court if necessary. It documents every person who has handled the evidence and ensures that it has not been tampered with.

NEW QUESTION: 284
What is the MOST effective way to detect installation of unauthorized software packages by employees?
A. Regular scanning of hard drives
B. Logging of activity on the network
C. Maintaining current antivirus software
D. Communicating the policy to employees
Answer: (SHOW ANSWER)

NEW QUESTION: 285
A senior auditor is reviewing work papers prepared by a junior auditor indicating that a finding was removed after the auditee said they corrected the problem. Which of the following is the senior auditor's MOST appropriate course of action?
A. Ask the auditee to retest.
B. Have the finding reinstated.
C. Refer the issue to the audit director.
D. Approve the work papers as written.
Answer: (SHOW ANSWER)

NEW QUESTION: 286
Which of the following is MOST important to include when developing an organization's test strategy?
A. Risks and contingencies
B. Test scenario benchmarks
C. Programming walk-throughs
D. Results of regression test
Answer: A (LEAVE A REPLY)
The most important aspect to include when developing an organization's test strategy is identifying risks and contingencies. This allows for proactive planning to address potential issues during testing, ensuring that the strategy accounts for unforeseen challenges and has appropriate mitigation measures in place to minimize disruption.

NEW QUESTION: 287
Which of the following should be the FIRST step in a data migration project?
A. Creating data conversion scripts
B. Understanding the new system's data structure
C. Completing data cleanup in the current database to eliminate inconsistencies
D. Reviewing decisions on how business processes should be conducted in the new system
Answer: (SHOW ANSWER)

NEW QUESTION: 288
Which of the following is the BEST way to mitigate risk to an organization's network associated with devices permitted under a bring your own device (BYOD) policy?
A. Ensure the policy requires antivirus software on devices.
B. Require personal devices to be reviewed by IT staff.
C. Implement a network access control system.
D. Enable port security on all network switches.
Answer: (SHOW ANSWER)

NEW QUESTION: 289

An IS auditor evaluating the change management process must select a sample from the change log. What is the BEST way for the auditor to confirm the change log is complete?

A. Obtain management attestation of completeness.

B. Take the last change from the system and trace it back to the log.

C. Take an item from the log and trace it back to the system.

D. Interview change management personnel about completeness.

Answer: (SHOW ANSWER)

https://ecampusontario.pressbooks.pub/auditinginformationsystems/chapter/0503/

NEW QUESTION: 290

Which of the following is the PRIMARY benefit of operational log management?

A. It enhances user experience via predictive analysis.

B. It improves security with real-time monitoring of network data.

C. It organizes data to identify performance issues.

D. It supports data aggregation using unified storage.

Answer: (SHOW ANSWER)

https://www.crowdstrike.com/cybersecurity-101/observability/log-management/

NEW QUESTION: 291

When determining the quality of evidence collected during an audit, it is MOST important to ensure the evidence is:

A. Valid, complete, and accurate.

B. Timely, reliable, and reasonable.

C. Sufficient and comes from the source of the information.

D. Persuasive and applicable.

Answer: (SHOW ANSWER)

ISACA defines sufficient and appropriate evidence as the standard for audit conclusions. Appropriateness relates to relevance (applicability) and reliability (persuasiveness). Evidence that is persuasive and directly applicable to the audit objective provides stronger assurance than evidence that is merely timely, complete, or reasonable. While the other options describe desirable qualities, they do not encompass the full ISACA standard. Thus, the most complete characterization of quality evidence is that it must be persuasive and applicable to the audit's purpose.

NEW QUESTION: 292

An IS auditor is providing input to an RFP to acquire a financial application system. Which of the following is MOST important for the auditor to recommend?

A. The application should meet the organization's requirements.

B. Potential suppliers should have experience in the relevant area.

C. Audit trails should be included in the design.

D. Vendor employee background checks should be conducted regularly.

Answer: (SHOW ANSWER)

NEW QUESTION: 293
An IS auditor has been tasked with analyzing an organization's capital expenditures against its repair and maintenance costs. Which of the following is the BEST reason to use a data analytics tool for this purpose?
A. It reduces the sample size required to perform the audit.
B. It reduces the error rate.
C. It improves the reliability of the data.
D. It enables the auditor to work with 100% of the transactions.
Answer: (SHOW ANSWER)

NEW QUESTION: 294
Which of the following should be an IS auditor's PRIMARY focus when auditing the implementation of a new IT operations performance monitoring system?
A. Validating whether baselines have been established
B. Reviewing whether all changes have been implemented
C. Determining whether there is a process for annual review of the maintenance manual
D. Confirming whether multi-factor authentication (MFA) is deployed as part of the operational enhancements
Answer: (SHOW ANSWER)
https://www.isaca.org/resources/isaca-journal/past-issues/2014/is-audit-basicsthe-core-of-it-auditing

NEW QUESTION: 295
Which of the following is the GREATEST advantage of vulnerability scanning over penetration testing?
A. The testing process can be automated to cover large groups of assets
B. Network bandwidth is utilized more efficiently
C. Custom-developed applications can be tested more accurately
D. The testing produces a lower number of false positive results
Answer: (SHOW ANSWER)

NEW QUESTION: 296
The waterfall life cycle model of software development is BEST suited for which of the following situations?
A. The project is subject to time pressures.
B. The project will involve the use of new technology.
C. The project intends to apply an object-oriented design approach.
D. The project requirements are well understood.
Answer: (SHOW ANSWER)

NEW QUESTION: 297
Which of the following would be of GREATEST concern to an IS auditor when assessing the effectiveness of log management?
A. Logs are stored on the same server as the application.
B. Logs are inconsistent.
C. The log reading utility tool is outdated.
D. Logs are not in a human-readable format.
Answer: (SHOW ANSWER)
Storing logs on the same server as the application poses the greatest risk because if the server is compromised, both the application and its logs could be altered or destroyed. This undermines the integrity and reliability of audit evidence needed for incident detection and forensic analysis.

NEW QUESTION: 298
An IS auditor is asked to provide feedback on the systems options analysis for a new project. The BEST course of action for the IS auditor would be to:
A. Identify the best alternative.
B. Retain comments as findings for the audit report.
C. Comment on the criteria used to assess the alternatives.
D. Request at least one other alternative.
Answer: (SHOW ANSWER)
The IS auditor should remain independent and objective. The best way to provide value without interfering in management decisions is to review and comment on the criteria used for evaluating alternatives, ensuring they are complete, relevant, and aligned with business needs.
Option A: Identifying the "best" option compromises independence.
Option B: Deferring to the audit report misses the chance to add timely value.
Option D: Requesting another alternative intrudes on management's role.
Option C: Correct - ensures appropriate evaluation criteria without biasing decisions.

NEW QUESTION: 299
Which of the following is the GREATEST advantage of utilizing guest operating systems in a virtual environment?
A. They prevent access to the greater environment via Transmission Control Protocol/Internet Protocol (TCP/IP)
B. They can be wiped quickly in the event of a security breach.
C. They are easier to containerize with minimal impact to the rest of the environment
D. They can be logged into and monitored from any location.
Answer: (SHOW ANSWER)

NEW QUESTION: 300

When collecting digital data for forensic purposes, the GREATEST benefit associated with the use of imaging is that it:

A. provides a bit-by-bit copy of original data and corrupted files for analysis
B. provides investigators with effective data visualizations
C. does not reproduce extraneous data, such as that from residual slack data and fragments
D. provides real-time disk mirroring capability for preventing forensic data loss
Answer: (SHOW ANSWER)
The greatest benefit of using imaging in forensic data collection is that it provides a bit-by-bit copy of the original data, including corrupted files, ensuring an exact replica of the storage medium for thorough analysis without altering the original evidence.

NEW QUESTION: 301
An IS auditor is reviewing an organization's risk management program. Which of the following should be the PRIMARY driver of the enterprise IT risk appetite?
A. Return on investment (ROI)
B. Cost of implementing controls
C. Strategic objectives
D. Likelihood of risk events
Answer: (SHOW ANSWER)
The organization's strategic objectives are the primary driver of its IT risk appetite because risk tolerance must align with the overall business strategy. This ensures that risk-taking supports the achievement of strategic goals while maintaining an acceptable level of exposure.

NEW QUESTION: 302
A finance group recently implemented new technologies and processes. Which type of IS audit would provide the GREATEST level of assurance that the department's objectives have been met?
A. Performance audit
B. Integrated audit
C. Financial audit
D. Cyber audit
Answer: (SHOW ANSWER)

NEW QUESTION: 303
When reviewing whether IT investments are meeting business objectives, which of the following evaluations would be MOST useful?
A. Realized return on investment (ROI) versus projected ROI
B. Actual return on investment (ROI) versus industry average ROI
C. A break-even analysis
D. Budgeted spend versus actual spend
Answer: A (LEAVE A REPLY)
The most useful evaluation when reviewing whether IT investments are meeting business objectives is comparing the realized return on investment (ROI) versus the projected ROI. This comparison helps assess whether the IT investment is delivering the expected benefits and aligning with the organization's objectives, providing insight into the effectiveness and value of the investment.

NEW QUESTION: 304
Which of the following establishes the PRIMARY difference between a business continuity plan (BCP) and a disaster recovery plan (DRP)?
A. The annual testing requirements
B. The timeframe for plan activation
C. The focus on system recovery
D. The involvement of senior management
Answer: (SHOW ANSWER)
The primary difference between a business continuity plan (BCP) and a disaster recovery plan (DRP) is that the BCP focuses on ensuring the continued operation of the business as a whole during disruptions, while the DRP specifically focuses on recovering IT systems and data after a disaster.

NEW QUESTION: 305
Which of the following is the BEST control to help ensure the completeness of outbound transactions?
A. Ensure the validity of the recipient ID and use auto-numbered reports
B. Verify transactions are sequentially numbered in the header record
C. Perform edit checks to identify erroneous, unusual, or valid transactions
D. Maintain a log of the number of messages are sent and validated periodically
Answer: (SHOW ANSWER)
Embedding and checking sequential numbers in the file or message header allows the system to automatically detect any missing or out-of-order transactions, directly supporting the completeness of outbound data flows.