[May-2022Valid Braindump2go CISM Exam PDF and VCE Dumps CISM 1959Q Offer[Q1890-Q1928

May/2022 Latest Braindump2go CISM Exam Dumps with PDF and VCE Free Updated Today! Following are some new CISM Real Exam Questions!QUESTION 1890The PRIMARY advantage of single sign-on (SSO) is that it will:A. increase the security of related applications.B. support multiple authentication mechanisms.C. increase efficiency of access management.D. strengthen user passwords.Answer: CQUESTION 1891Which of the following would provide the MOST useful information when prioritizing controls to be added to a system?A. Baseline to industry standardsB. The risk registerC. Balanced scorecardD. Compliance requirementsAnswer: BQUESTION 1892An organization has recently acquired a smaller company located in a different geographic region.Which of the following is the BEST approach for addressing conflicts between the parent organization's security standards and local regulations affecting the acquired company?A. Adopt the standards of the newly acquired company.B. Give precedence to the parent organization's standards.C. Create a global version of the local regulations,D. Create a local version of the parent organization's standards.Answer: BQUESTION 1893An organization has decided to outsource its disaster recovery function. Which of the following is the MOST important consideration when drafting the service level agreement (SLA)?A. Recovery time objectives (RTOs)B. Testing requirementsC. Recovery point objectives (RPOs)D. Authorization chainAnswer: BQUESTION 1894Which of the following MOST effectively allows for disaster recovery testing without interrupting business operations?A. Full interruption testingB. Simulation testingC. Parallel testingD. Structured walk-throughAnswer: AQUESTION 1895When defining and communicating roles and responsibilities between an organization and cloud service provider, which of the following situations would present the GREATEST risk to the organization's ability to ensure information risk is managed appropriately?A. The Service agreement results in unnecessary duplication of effort because shared responsibilities have not been clearly defined.B. The organization and provider identified multiple information security responsibilities that neither party was planning to provide.C. The service agreement uses a custom-developed RACI instead of an industry standard RACI to document responsibilities.D. The organization believes the provider accepted responsibility for issues affecting security that the provider did not accept.Answer: DQUESTION 1896An organization has implemented a new security control in response to a recently discovered vulnerability. Several employees have voiced concerns that the control disrupts their ability to work. Which of the following is the information security manager's BEST course of action?A. Educate users about the vulnerability.B. Report the control risk to senior management.C. Accept the vulnerability.D. Evaluate compensating control options.Answer: DQUESTION 1897An incident response team recently encountered an unfamiliar type of cyber event. Though the team was able to resalve the issue, it took a significant amount of time to identify, What is the BEST way to help ensure similar incidents are identified more quickly in the future?A. Implement a SIEM solution.B. Perform a post-incident review.C. Perform a threat analysis.D. Establish performance metrics for the team.Answer: BQUESTION 1898An organization's ClO has tasked the information security manager with drafting the charter for an information security steering committee. The committee will be comprised of the C/O, the IT shared services manager, the vice president of marketing, and the information security manager. Which of the following is the MOST significant issue with the development of this committee?A. The CIO is not taking charge of the committee.B. There is a conflict of interest between the business and IT.C. The committee lacks sufficient business representation.D. The committee consists of too many senior executives.Answer: CQUESTION 1899Which of the following is MOST important to ensure when considering exceptions to an information security policy?A. Exceptions are based on data classification.B. Exceptions undergo regular review.C. Exceptions reflect the organizational risk appetite.D. Exceptions are approved by executive management.Answer: CQUESTION 1900Which of the following would be MOST useful in determining how an organization will be affected by a new regulatory requirement for cloud services?A. Risk assessmentB. Data classification policyC. Information asset inventoryD. Data loss protection planAnswer: AQUESTION 1901Which of the following is an information security manager's BEST course of action upon discovering an organization with budget constraints lacks several important security capabilities?A. Suggest the deployment of open-source security tools to mitigate identified risks.B. Recommend that the organization avoid the most severe risks.C. Establish a business case to demonstrate return on investment (ROI) of a security tool.D. Review the most recent audit report and request funding to address the most serious finding.Answer: CQUESTION 1902Which of the following is the BEST way to strengthen the alignment of an information security program with business strategy?A. Providing organizational training on information security policiesB. Increasing budget for risk assessmentsC. Increasing the frequency of control assessmentsD. Establishing an information security steering committeeAnswer: DQUESTION 1903Which of the following is the PRIMARY responsibility of an information security governance committee?A. Approving changes to the information security strategyB. Discussing upcoming information security

projectsC. Reviewing monthly information security metricsD. Reviewing the information security risk registerAnswer: AQUESTION 1904An organization has established a bring your own device (BYOD) program. Which of the following is the MOST important security consideration when allowing employees to use personal devices for corporate applications remotely?A. Security awareness trainingB. Secure application developmentC. Mobile operating systems supportD. Mandatory controls for maintaining security policyAnswer: AQUESTION 1905An organization is developing a disaster recovery strategy and needs to identify each application's criticality so that the recovery sequence can be established. Which of the following is the BEST course of action?A. Document the data flow and review the dependencies.B. Perform a business impact analysis (BIA) on each application.C. Restore the applications with the shortest recovery times first.D. Identify which applications contribute the most cash flow.Answer: BQUESTION 1906an information security manager has identified a major security event with potential noncompliance implications. Who should be notified FIRST?A. Internal auditB. Senior managementC. Public relations teamD. Regulatory authoritiesAnswer: BQUESTION 1907Which of the following should be the PRIMARY focus of a status report on the information security program to senior management?A. Demonstrating risk is managed at the desired levelB. Confirming the organization complies with security policiesC. Providing evidence that resources are performing as expectedD. Verifying security costs do not exceed the budgetAnswer: AQUESTION 1908To address the issue that performance pressures on IT may conflict with information security controls, itis MOST important that:A. the Steering committee provides guidance and dispute resolution.B. noncompliance issues are reported to senior management.C. IT policies and procedures are better aligned to security policies.D. the security policy is changed to accommodate IT performance pressure.Answer: AQUESTION 1909Which of the following would BEST help an organization's ability to manage advanced persistent threats (APT)?A. Using multiple security vendorsB. Having a skilled information security teamC. Having network detection tools in placeD. Increasing the information security budgetAnswer: CQUESTION 1910Priore implementing a bring your own device (BYOD) program, it is MOST important to:A. select mobile device management (MDM) software.B. survey employees for requested applications.C. review currently utilized applications.D. develop an acceptable use policy.Answer: DQUESTION 1911In an organization that has several independent security tools including intrusion detection systems (IDSs) and firewalls, which of the following is the BEST way to ensure timely detection of incidents?A. Ensure staff are cross trained to manage all security tools.B. Ensure that the incident response plan is endorsed by senior management.C. Outsource the management of security tools to a service provider.D. Implement a log aggregation and correlation solution.Answer: DQUESTION 1912Which of the following is the PRIMARY responsibility of an information security steering committee?A. Revigwing firewall rulesB. Setting up password expiration proceduresC. Prioritizing security initiativesD. Drafting security policiesAnswer: CQUESTION 1913Which of the following would be MOST helpful when determining appropriate access controls for an application?A. End-user inputB. Industry best practicesC. Data criticalityD. Gap analysis resultsAnswer: CQUESTION 1914Which of the following provides the MOST relevant information to determine the overall effectiveness of an information security program and underlying business processes?A. SWOT analysisB. Balanced scorecardC. Cost-benefit analysisD. Industry benchmarksAnswer: BQUESTION 1915What should be an information security manager's MOST important consideration when reviewing a proposed upgrade to a business unit's production database?A. Ensuring residual risk is within apbetiteB. Ensuring the application inventory is updatedC. Ensuring a cost-benefit analysis is completedD. Ensuring senior management is aware of associated riskAnswer: AQUESTION 1916Which of the following metrics provides the BEST measurement of the effectiveness of a security awareness program?A. Mean time between incident detection and remediationB. Variance of program cost to allocated budgetC. The number of reported security incidentsD. The number of security breachesAnswer: AQUESTION 1917Which of the following is an information security manager's FIRST priority after a high-profile system has been compromised?A. Implement improvements to prevent recurrence.B. Identify the malware that compromised the system.C. Preserve incident-related data.D. Restore the compromised system.Answer: DQUESTION 1918Which of the following should an information security manager do FIRST to address complaints that a newly implemented security control has slowed business operations?A. Discuss the issue with senior management for direction.B. Validate whether the control is operating as intended.C. Remove the control and identify alternatives.D. Conduct user awareness training.Answer: BQUESTION 1919An information security manager was informed that a planned penetration test could potentially disrupt some services.Which of the following should be the FIRST course of action?A. Ensure the service owner is available during the penetration test.B. Accept the risk and document it in the risk register.C. Estimate the impact and inform the business owner.D. Reschedule the activity during an approved maintenance window.Answer: CQUESTION 1920What is the PRIMARY objective of implementing standard security configurations?A. Maintain a flexible approach to mitigate potential risk to unsupported systems.B. Compare configurations between supported and unsupported systems.C. Minimize the operational burden of managing and monitoring unsupported systems.D. Control vulnerabilities and

reduce threats from changed configurations.Answer: DQUESTION 1921In addition to executive sponsorship and business alignment, which of the following is MOST critical for information security governance?A. Allocation of training resourcesB. Compliance with policiesC. Auditability of systemsD. Ownership of securityAnswer: DQUESTION 1922When developing an incident escalation process, the BEST approach is to classify incidents based on:A. estimated time to recover.B. information assets affected.C. their root causes.D. recovery point objectives (RPOs).Answer: DQUESTION 1923An employee clicked on a link in a phishing email, triggering a ransomware attack. Which of the following should be the information security manager's FIRST step?A. Wipe the affected system.B. lsolate the impacted endpoints.C. Notify senior management D. Notify internal legal counsel.Answer: BQUESTION 1924The PRIMARY purpose for defining key risk indicators (KRIs) for a security program is to:A. ensure mitigating controls meet specifications.B. provide information needed to take action.C. support investments in the security program.D. compare security program effectiveness to benchmarks.Answer: AQUESTION 1925An information security manager is preparing incident response plans for an organization that processes personal and financial information. Which of the Following is the MOST important consideration?A. Identifying regulatory requirementsB. Determining budgetary constraints.C. Aligning with enterprise architecture (EA)D. Aligning with an established industry frameworkAnswer: AQUESTION 1926To implement effective continuous monitoring of IT controls, an information security manager needs to FIRST ensure:A. security alerts are centralized.B. periodic scanning of IT systems is in place.C. metrics are communicated to senior management.D. information assets have been classified.Answer: CQUESTION 1927Which of the following is MOST likely to be included in an enterprise security policy?A. Retention schedulesB. Organizational riskC. System access specificationsD. Definitions of responsibilitiesAnswer: DQUESTION 1928Which of the following is the BEST way to build a risk-aware culture?A. Periodically test compliance with security controls and post results.B. Periodically change risk awareness messages.C. Ensure that threats are communicated organization-wide in a timely manner.D. Establish incentives and a channel for staff to report risks.Answer: AResources From:1.2022 Latest Braindump2go CISM Exam Dumps (PDF & VCE) Free Share: https://www.braindump2go.com/cism.html2.2022 Latest Braindump2go CISM PDF and CISM VCE Dumps Free Share: https://drive.google.com/drive/folders/1GQzdCXx8t3NzUvXsN8V7eoR3FXqRs-t6?usp=sharing3.2021 Free Braindump2go CISM Exam Questions Download:https://www.braindump2go.com/free-online-pdf/CISM-PDF(1704-1805).pdf https://www.braindump2go.com/free-online-pdf/CISM-PDF-Dumps(1603-1703).pdf https://www.braindump2go.com/free-online-pdf/CISM-VCE-Dumps(1806-1928).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!