[New Exam Dumps Real PassLeader 712-50 Braindumps And VCE Dumps Ensure 100 Percent Exam Passing

Where To Get The 100 Percent Valid 712-50 Exam Dumps? PassLeader -- one famous IT Certification Exam Study Materials Supplier -- is offer the 100 percent valid 350q 712-50 exam dumps, which covers all the new 712-50 exam questions with detailed explanation and it has been helped many people passing 712-50 exam easily! Welcome to choose the best 350q 712-50 practice test from passleader.com, both 712-50 PDF dumps and VCE dumps are available now! keywords: 350q 712-50 exam dumps,712-50 pdf dumps,712-50 braindumps,712-50 vce dumps,350q 712-50 exam questions,712-50 practice test,712-50 study guide,EC-Council Certified CISO (CCISO) Exam

QUESTION 1Information security policies should be reviewed: A.   by stakeholders at least annuallyB.   by the CISO when new systems are brought onlineC.   by the Incident Response team after an auditD.   by internal audit semiannually Answer: A QUESTION 2What role should the CISO play in properly scoping a PCI environment? A.   Validate the business units' suggestions as to what should be included in the scoping processB.   Work with a Qualified Security Assessor (QSA) to determine the scope of the PCI environmentC.   Ensure internal scope validation is completed and that an assessment has been done to discover all credit card dataD.   Complete the self-assessment questionnaire and work with an Approved Scanning Vendor (ASV) to determine scope Answer: C QUESTION 3A security professional has been promoted to be the CISO of an organization. The first task is to create a security policy for this organization. The CISO creates and publishes the security policy. This policy however, is ignored and not enforced consistently. Which of the following is the MOST likely reason for the policy shortcomings? A.   Lack of a formal security awareness programB.   Lack of a formal security policy governance processC.   Lack of formal definition of roles and responsibilitiesD.   Lack of a formal risk management policy Answer: B QUESTION 4When a CISO considers delaying or not remediating system vulnerabilities which of the following are MOST important to take into account? A.   Threat Level, Risk of Compromise, and Consequences of CompromiseB.   Risk Avoidance, Threat Level, and Consequences of CompromiseC.   Risk Transfer, Reputational Impact, and Consequences of CompromiseD.   Reputational Impact, Financial Impact, and Risk of Compromise Answer: A QUESTION 5As the new CISO at the company you are reviewing the audit reporting process and notice that it includes only detailed technical diagrams. What else should be in the reporting process? A.   Executive summaryB. Penetration test agreementC.   Names and phone numbers of those who conducted the auditD.   Business charter Answer: A QUESTION 6When a critical vulnerability has been discovered on production systems and needs to be fixed immediately, what is the BEST approach for a CISO to mitigate the vulnerability under tight budget constraints? A.   Transfer financial resources from other critical programsB.   Take the system off line until the budget is availableC.   Deploy countermeasures and compensating controls until the budget is availableD.   Schedule an emergency meeting and request the funding to fix the issue Answer: C QUESTION 7The executive board has requested that the CISO of an organization define and Key Performance Indicators (KPI) to measure the effectiveness of the security awareness program provided to call center employees. Which of the following can be used as a KPI? A.   Number of callers who report security issues.B.   Number of callers who report a lack of customer service from the call centerC.   Number of successful social engineering attempts on the call centerD.   Number of callers who abandon the call before speaking with a representative Answer: C QUESTION 8Many times a CISO may have to speak to the Board of Directors (BOD) about their cyber security posture. What would be the BEST choice of security metrics to present to the BOD? A.   All vulnerabilities found on servers and desktopsB.   Only critical and high vulnerabilities on servers and desktopsC.   Only critical and high vulnerabilities that impact important production serversD.   All vulnerabilities that impact important production servers Answer: C QUESTION 9Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage? A.   Servers, routers, switches, modemB.   Firewall, exchange, web server, intrusion detection system (IDS)C.   Firewall, anti-virus console, IDS, syslogD.   IDS, syslog, router, switches Answer: C QUESTION 10A new CISO just started with a company and on the CISO's desk is the last complete Information Security Management audit report. The audit report is over two years old. After reading it, what should be the CISO's FIRST priority? A.

Have internal audit conduct another audit to see what has changed.B.   Contract with an external audit company to conduct an unbiased auditC.   Review the recommendations and follow up to see if audit implemented the changesD.   Meet with audit team to determine a timeline for corrections Answer: C QUESTION 11To have accurate and effective information security policies how often should the CISO review the organization policies? A.   Every 6 monthsB.   QuarterlyC.   Before an auditD.   At least once a year Answer: D QUESTION 12As a new CISO at a large healthcare company you are told that everyone has to badge in to get in the building. Below your office window you notice a door that is normally propped open during the day for groups of people to take breaks outside. Upon looking closer you see there is no badge reader. What should you do? A.   Nothing, this falls outside your area of influence.B.   Close and chain the door shut and send a company-wide memo banning the practice.C.   Have a risk assessment performed.D.   Post a guard at the door to maintain physical security. Answer: C