[2017 New Exam Collection SY0-401 Dumps And SY0-401 New Questions (226-250)

2017 August CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!
2017 timesaving comprehensive guides for CompTIA SY0-401 exam: Using latest released Lead2pass SY0-401 exam questions, quickly pass SY0-401 exam 100%! Following questions and answers are all new published by CompTIA Official Exam Center! Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 226A security administrator wants to deploy a physical security control to limit an individual's access into a sensitive area. Which of the following should be implemented? A. GuardsB. CCTVC. BollardsD. Spike stripAnswer: AExplanation:A guard can be intimidating and respond to a situation and in a case where you want to limit an individual's access to a sensitive area a guard would be the most effective. QUESTION 227After running into the data center with a vehicle, attackers were able to enter through the hole in the building and steal several key servers in the ensuing chaos. Which of the following security measures can be put in place to mitigate the issue from occurring in the future? A. FencingB. Proximity readersC. Video surveillanceD. Bollards Answer: DExplanation:To stop someone from entering a facility, barricades or gauntlets can be used. These are often used in conjunction with guards, fencing, and other physical security measures. Bollards are physical barriers that are strong enough to withstand impact with a vehicle. QUESTION 228A system administrator has concerns regarding their users accessing systems and secured areas using others' credentials. Which of the following can BEST address this concern? A. Create conduct policies prohibiting sharing credentials.B. Enforce a policy shortening the credential expiration timeframe.C. Implement biometric readers on laptops and restricted areas.D. Install security cameras in areas containing sensitive systems. Answer: CExplanation:Biometrics is an authentication process that makes use of physical characteristics to establish identification. This will prevent users making use of others credentials. QUESTION 229Which of the following preventative controls would be appropriate for responding to a directive to reduce the attack surface of a specific host? A. Installing anti-malwareB. Implementing an IDSC. Taking a baseline configurationD. Disabling unnecessary services Answer: DExplanation:Preventive controls are to stop something from happening. These can include locked doors that keep intruders out, user training on potential harm (to keep them vigilant and alert), or even biometric devices and guards that deny access until authentication has occurred. By disabling all unnecessary services you would be reducing the attack surface because then there is less opportunity for risk incidents to happen. There are many risks with having many services enabled since a service can provide an attack vector that someone could exploit against your system. It is thus best practice to enable only those services that are absolutely required. QUESTION 230Joe, the system administrator, has been asked to calculate the Annual Loss Expectancy (ALE) for a $5,000 server, which often crashes. In the past year, the server has crashed 10 times, requiring a system reboot to recover with only 10% loss of data or function. Which of the following is the ALE of this server? A. $500B. $5,000C. $25,000D. $50,000 Answer: BExplanation:SLE × ARO = ALE, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.(5000 x 10) x 0.1 = 5000 QUESTION 231Sara, a security analyst, is trying to prove to management what costs they could incur if their customer database was breached. This database contains 250 records with PII. Studies show that the cost per record for a breach is $300. The likelihood that their database would be breached in the next year is only 5%.Which of the following is the ALE that Sara should report to management for a security breach? A. $1,500B. $3,750C. $15,000D. $75,000 Answer: BExplanation:SLE × ARO = ALE, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.SLE = 250 x $300; ARO = 5%$75000 x 0.05 = $3750 QUESTION 232An advantage of virtualizing servers, databases, and office applications is: A. Centralized management.B. Providing greater resources to users.C. Stronger access control.D. Decentralized management. Answer: AExplanation:Virtualization consists of allowing one set of hardware to host multiple virtual Machines and in the case of software and applications; one host is all that is required. This makes centralized management a better prospect. QUESTION 233Key elements of a business impact analysis should include which of the following tasks? A. Develop recovery strategies, prioritize recovery, create test plans, post-test evaluation, and update processes.B. Identify institutional and regulatory reporting requirements, develop response teams and communication trees, and develop press release templates.C. Employ regular preventive measures such as patch management, change management, antivirus and vulnerability scans, and reports to management.D. Identify critical assets systems and functions, identify dependencies, determine critical downtime limit, define scenarios by type and scope of impact, and quantify loss potential. Answer: DExplanation:The key components of a Business impact analysis (BIA) include:Identifying Critical FunctionsPrioritizing Critical Business Functions Calculating a Timeframe for Critical Systems LossEstimating the Tangible and Intangible Impact on the Organization QUESTION 234A security administrator is tasked with calculating the total ALE on servers. In a two year period of time, a company has to

replace five servers. Each server replacement has cost the company $4,000 with downtime costing $3,000. Which of the following is the ALE for the company? A. $7,000B. $10,000C. $17,500D. $35,000 Answer: CExplanation:SLE × ARO = ALE, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.SLE =($4000 + $3000) x 5 = $35000ARO = 2 years Thus per year it would be 50% = 0,5The ALE is thus $35000 x 0.5 = $17500 QUESTION 235In the case of a major outage or business interruption, the security office has documented the expected loss of earnings, potential fines and potential consequence to customer service. Which of the following would include the MOST detail on these objectives? A. Business Impact AnalysisB. IT Contingency PlanC. Disaster Recovery PlanD. Continuity of Operations Answer: A Explanation:Business impact analysis (BIA) is the process of evaluating all of the critical systems in an organization to define impact and recovery plans. BIA isn't concerned with external threats or vulnerabilities; the analysis focuses on the impact a loss would have on the organization. A BIA comprises the following: identifying critical functions, prioritizing critical business functions, calculating a timeframe for critical systems loss, and estimating the tangible impact on the organization. QUESTION 236 Which of the following would BEST be used to calculate the expected loss of an event, if the likelihood of an event occurring is known? (Select TWO). A. DACB. ALEC. SLED. AROE. ROI Answer: BCExplanation:ALE (Annual Loss Expectancy) is equal to the SLE (Single Loss Expectancy) times the annualized rate of occurrence. SLE (Single Loss Expectancy) is equal to asset value (AV) times exposure factor (EF). QUESTION 237A company's chief information officer (CIO) has analyzed the financial loss associated with the company's database breach. They calculated that one single breach could cost the company $1,000,000 at a minimum. Which of the following documents is the CIO MOST likely updating? A. Succession planB. Continuity of operation planC. Disaster recovery planD. Business impact analysis Answer: DExplanation:Business impact analysis (BIA) is the process of evaluating all of the critical systems in an organization to define impact and recovery plans. BIA isn't concerned with external threats or vulnerabilities; the analysis focuses on the impact a loss would have on the organization. A BIA comprises the following: identifying critical functions, prioritizing critical business functions, calculating a timeframe for critical systems loss, and estimating the tangible impact on the organization. QUESTION 238A network administrator has recently updated their network devices to ensure redundancy is in place so that: A. switches can redistribute routes across the network.B. environmental monitoring can be performed.C. single points of failure are removed.D. hot and cold aisles are functioning. Answer: CExplanation:Redundancy refers to systems that either are duplicated or fail over to other systems in the event of a malfunction. The best way to remove an SPOF from your environment is to add redundancy. QUESTION 239After an assessment, auditors recommended that an application hosting company should contract with additional data providers for redundant high speed Internet connections. Which of the following is MOST likely the reason for this recommendation? (Select TWO). A. To allow load balancing for cloud supportB. To allow for business continuity if one provider goes out of businessC. To eliminate a single point of failureD. To allow for a hot site in case of disasterE. To improve intranet communication speeds Answer: BCExplanation:A high-speed internet connection to a second data provider could be used to keep an up-to-date replicate of the main site. In case of problem on the first site, operation can quickly switch to the second site. This eliminates the single point of failure and allows the business to continue uninterrupted on the second site.Note: Recovery Time ObjectiveThe recovery time objective (RTO) is the maximum amount of time that a process or service is allowed to be down and the consequences still be considered acceptable. Beyond this time, the break in business continuity is considered to affect the business negatively. The RTO is agreed on during BIA creation. QUESTION 240Which of the following utilities can be used in Linux to view a list of users' failed authentication attempts? A. badlogB. faillogC. wronglogD. killlog Answer: BExplanation:var/log/faillog - This Linux log fi le contains failed user logins. You'll find this log useful when tracking attempts to crack into your system./var/log/apport.log This log records application crashes. Sometimes these can reveal attempts to compromise the system or the presence of a virus or spyware. QUESTION 241Which of the following risks could IT management be mitigating by removing an all-in-one device? A. Continuity of operationsB. Input validationC. Single point of failureD. Single sign on Answer: CExplanation:The major disadvantage of combining everything into one, although you do this to save costs, is to include a potential single point of failure and the reliance/dependence on a single vendor. QUESTION 242Which of the following risk concepts requires an organization to determine the number of failures per year? A. SLEB. ALEC. MTBFD. Quantitative analysis Answer: BExplanation:ALE is the annual loss expectancy value. This is a monetary measure of how much loss you could expect in a year. QUESTION 243Upper management decides which risk to mitigate based on cost. This is an example of: A. Qualitative risk assessmentB. Business impact analysisC. Risk management frameworkD. Quantitative risk assessment Answer: DExplanation:Quantitative analysis / assessment is used to the show the logic and cost savings in replacing a server for example before it fails rather than after the failure. Quantitative assessments assign a dollar amount. QUESTION 244Corporate IM presents multiple concerns to enterprise IT. Which of the following concerns should Jane, the IT security manager, ensure are under control? (Select THREE). A. AuthenticationB. Data leakageC. ComplianceD. MalwareE. Non-repudiationF. Network

loading Answer: BCDExplanation:In a joint enterprise, data may be combined from both organizations. It must be determined, in advance, who is responsible for that data and how the data backups will be managed. Data leakage, compliance and Malware issues are all issues concerning data ownership and backup which are both impacted on by corporate IM. QUESTION 245Which of the following is being tested when a company's payroll server is powered off for eight hours? A. Succession planB. Business impact documentC. Continuity of operations planD. Risk assessment plan Answer: CExplanation:Continuity of operations plan is the effort to ensure the continued performance of critical business functions during a wide range of potential emergencies. QUESTION 246A security administrator is reviewing the company's continuity plan. The plan specifies an RTO of six hours and RPO of two days. Which of the following is the plan describing? A. Systems should be restored within six hours and no later than two days after the incident.B. Systems should be restored within two days and should remain operational for at least six hours.C. Systems should be restored within six hours with a minimum of two days worth of data.D. Systems should be restored within two days with a minimum of six hours worth of data. Answer: CExplanation:The recovery time objective (RTO) is the maximum amount of time that a process or service is allowed to be down and the consequences still to be considered acceptable. Beyond this time, the break in business continuity is considered to affect the business negatively. The RTO is agreed on during the business impact analysis (BIA) creation.The recovery point objective (RPO) is similar to RTO, but it defines the point at which the system needs to be restored. This could be where the system was two days before it crashed (whip out the old backup tapes) or five minutes before it crashed (requiring complete redundancy). As a general rule, the closer the RPO matches the item of the crash, the more expensive it is to obtain. QUESTION 247Pete, the system administrator, is reviewing his disaster recovery plans. He wishes to limit the downtime in the event of a disaster, but does not have the budget approval to implement or maintain an offsite location that ensures 99.99% availability. Which of the following would be Pete's BEST option? A. Use hardware already at an offsite location and configure it to be quickly utilized.B. Move the servers and data to another part of the company's main campus from the server room.C. Retain data back-ups on the main campus and establish redundant servers in a virtual environment.D. Move the data back-ups to the offsite location, but retain the hardware on the main campus for redundancy. Answer: AExplanation:A warm site provides some of the capabilities of a hot site, but it requires the customer to do more work to become operational. Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations. For most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement. Warm sites may be for your exclusive use, but they don't have to be. A warm site requires more advanced planning, testing, and access to media for system recovery. Warm sites represent a compromise between a hot site, which is very expensive, and a cold site, which isn't preconfigured. QUESTION 248Ann is starting a disaster recovery program. She has gathered specifics and team members for a meeting on site. Which of the following types of tests is this? A. Structured walkthroughB. Full Interruption testC. Checklist testD. Tabletop exercise Answer: AExplanation:A structured walkthrough test of a recovery plan involves representatives from each of the functional areas coming together to review the plan to determine if the plan pertaining to their area is accurate and complete and can be implemented when required. QUESTION 249 When a communications plan is developed for disaster recovery and business continuity plans, the MOST relevant items to include would be: (Select TWO). A. Methods and templates to respond to press requests, institutional and regulatory reporting requirements.B. Methods to exchange essential information to and from all response team members, employees, suppliers, and customers.C. Developed recovery strategies, test plans, post-test evaluation and update processes.D. Defined scenarios by type and scope of impact and dependencies, with quantification of loss potential.E. Methods to review and report on system logs, incident response, and incident handling. Answer: ABExplanation:A: External emergency communications that should fit into your business continuity plan include notifying family members of an injury or death, discussing the disaster with the media, and providing status information to key clients and stakeholders. Each message needs to be prepared with the audience (e.g., employees, media, families, government regulators) in mind; broad general announcements may be acceptable in the initial aftermath of an incident, but these will need to be tailored to the audiences in subsequent releases.B: A typical emergency communications plan should be extensive in detail and properly planned by a business continuity planner. Internal alerts are sent using either email, overhead building paging systems, voice messages or text messages to cell/smartphones with instructions to evacuate the building and relocate at assembly points, updates on the status of the situation, and notification of when it's safe to return to work. QUESTION 250After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service? A. Succession planningB. Disaster recovery planC. Information security planD. Business impact analysis Answer: BExplanation:A disaster-recovery plan, or scheme, helps an organization respond effectively when a disaster occurs. Disasters may include system failure, network failure, infrastructure failure, and natural disaster. The primary emphasis of such a plan is reestablishing services and minimizing losses. Lead2pass is confident that our NEW UPDATED

SY0-401 exam questions and answers are changed with CompTIA Official Exam Center. If you cannot pass SY0-401 exam, never mind, we will return your full money back! Visit Lead2pass exam dumps collection website now and download SY0-401 exam dumps instantly today! SY0-401 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDVzFZWExUbFM0YU0 2017 CompTIA **SY0-401** exam dumps (All 1868 Q&As) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]