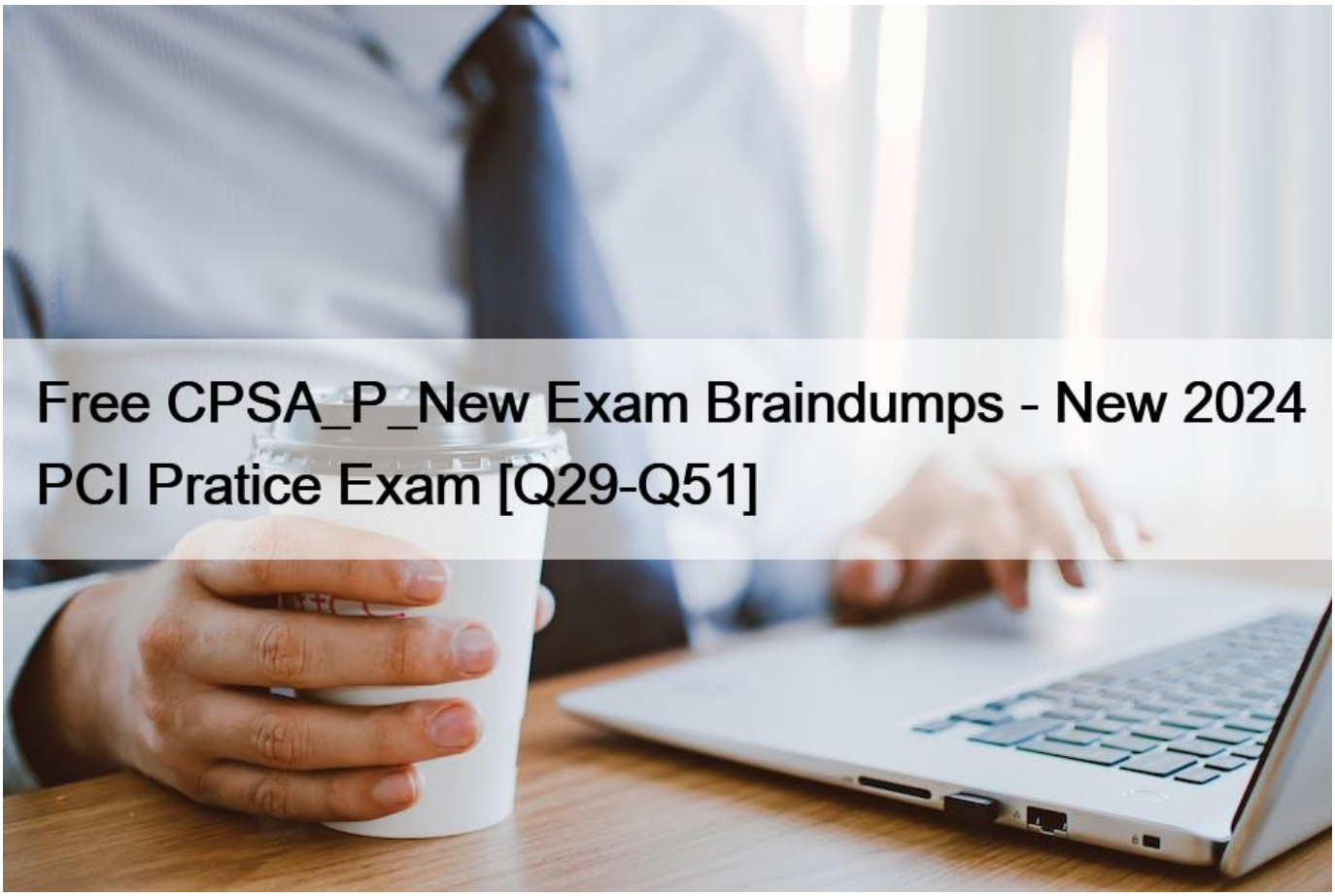
Free CPSA_P_New Exam Braindumps - New 2024 PCI Pratice Exam [Q29-Q51



Free CPSA_P_New Exam Braindumps - New 2024 PCI Pratice Exam
Practice Test for CPSA_P_New Certification Real 2024 Mock Exam

Q29. In which of the following locations must the CCTV and access control servers be located?
* Within the Security Control Room (SCR)
* Within a room in the HSA with security controls equivalent to the SCR applied
* Within the SCR or a room with equivalent security
* Within the secure server room inside of the HSA

Explanation

According to the PCI Card Production Physical Security Requirements, the CCTV and access control servers must be located within the Security Control Room (SCR) or a room with equivalent security. This means that the room must have the same level of physical protection as the SCR, such as locks, alarms, sensors, cameras, and access control devices. The purpose of this requirement is to prevent unauthorized access, tampering, or theft of the servers that store and process sensitive data related to card production and security. References: PCI Card Production Physical Security Requirements, v2.0, April 2019, page 16

Q30. Which of the following must be used by the vendor to protect doors that provide access to buildings containing air conditioning equipment?

* Security tape that will leave an observable trace each time a door is opened
* Electrical contacts that log each open and close event to a secure system memory
* Magnetic contacts that are permanently alarmed and that are connected to the security control-room panels
* Physical locks with a limited set of keys under constant supervision by a guard in the security control-room

Explanation

According to the PCI Card Production and Provisioning Physical Security Requirements, the vendor must use magnetic contacts that are permanently alarmed and that are connected to the security control-room panels to protect doors that provide access to buildings containing air conditioning equipment. The vendor must also ensure that the air conditioning equipment is located in a secure area that is not accessible to unauthorized personnel, and that the air conditioning system is monitored and maintained to prevent unauthorized access or tampering. The vendor must also have procedures to respond to any alarms or incidents related to the air conditioning system, and to report them to the relevant parties. The vendor must not use security tape, electrical contacts, or physical locks alone, as these may not provide adequate protection or detection of unauthorized access or tampering. References: PCI Card Production and Provisioning Physical Security Requirements and Test Procedures v3.0, January 2022, pages 21-221

Q31. Which of these is a requirement of the security control room?

* Access must be controlled by a physical key (in case of power-failure)
* Access must be monitored in real-time
* At least one guard must be present at all times
* Dual-control must be used to grant entry

Explanation

According to the PCI Card Production and Provisioning Physical Security Requirements, the security control room is the area where the security systems are monitored and controlled. The requirement for the security control room is that access must be monitoredin real-time by a guard or an automated system that alerts the guard of any unauthorized access attempts. The security control room must also be protected by physical barriers and access control devices that prevent unauthorized entry. The other options are not requirements of the security control room, although they may be implemented as additional security measures. References:

PCI Card Production and Provisioning Physical Security Requirements, Version 1.0, April 2019, page

151

PCI Card Production and Provisioning Physical Security Requirements, Version 1.0, April 2019, page

161

Q32. Which of the following must every assessor do to maintain their CPSA certification?

* Complete annual requalification training or complete 3 assessments for different facilities each year
* Earn and document at least 20 hours of Continuing Professional Education (CPE) over 3 years
* Earn an additional professional certification from List A or B of the Qualification Requirements (QRs)
* Submit evidence of internal training in a relevant area (as per the QRs)

Explanation

According to the Card Production Security Assessor (CPSA) Qualification Requirements, CPSAs must maintain their qualification status by either completing the annual requalification training provided by PCI SSC or performing at least three (3) PCI Card Production Assessments for different facilities over the previous one-year period. This ensures that CPSAs remain current with technical and industry changes and demonstrate professionalism. References: Card Production Security Assessor (CPSA) Qualification Requirements, v1.1, March 2022, page 10

Q33. A vendor discovers that a recent shipment of cards is missing a set. Which of the following responses would you expect in a

compliant organization?
* An immediate call is made to the issuer and the VPA who, between them, contact law enforcement and put together a joint statement
* The head of security initiates a meeting, and once the VPA approves the messaging, law enforcement is notified in two days
* A report is requested by the issuer, the vendor sends it to them, and the issuer handles the incident with the local police
* After an incident review, the VPA, issuer and law enforcement are all notified within 24 hours
Explanation

According to the PCI Card Production Physical Security Requirements, one of the security controls for card shipment is to ensure that the vendor has an incident response plan in place to handle any card shipment incidents, such as loss, theft, or tampering. The incident response plan should include the following steps1:

The vendor should conduct an incident review to determine the cause and scope of the incident, and document the findings and actions taken.

The vendor should notify the VPA, the issuer, and law enforcement of the incident within 24 hours of discovery, or as soon as possible.

The vendor should cooperate with the VPA, the issuer, and law enforcement in the investigation and resolution of the incident, and provide any evidence or information requested.

The vendor should implement corrective actions to prevent the recurrence of the incident, and report the results to the VPA and the issuer. Therefore, the response that best reflects a compliant organization is option D, which follows the steps of the incident response plan as required by the PCI Card Production Physical Security Requirements. References: PCI Card Production Physical Security Requirements, Version 1.0, April 2019, Section 1.1, Objective 6, Requirement 6.2, Page 131

Q34. Before you go on-site, the vendor’s primary contact communicates a legitimate reason for delaying the assessment for several months. Who can approve the change in the report delivery schedule?
* Vendor senior management
* Payment brands
* Affected issuers
* PCI SSC
Explanation

According to the PCI CPSA Qualification Requirements, one of the administrative requirements for CPSA Companies is to adhere to the report delivery schedule as defined by the PCI SSC. The report delivery schedule specifies the deadlines for submitting the PCI Card Production Reports on Compliance (ROCs) and Attestations of Compliance (AOCs) to the PCI SSC and the payment brands. The report delivery schedule also defines the circumstances under which a CPSA Company may request an extension or a waiver of the report delivery deadline. The PCI SSC is the only entity that can approve the change in the report delivery schedule, and the CPSA Company must submit a written request to the PCI SSC with a valid reason for the delay and the proposed new delivery date. The PCI SSC will review the request and notify the CPSA Company of its decision. The PCI SSC may also notify the payment brands and the affected issuers of the change in the report delivery schedule. References: PCI CPSA Qualification Requirements, Version 1.1, April 2020, Section 6.1.4, Page 121

Q35. To liberate a person detected inside of the inner shipping delivery room and stop the alarm, the software monitoring the access-control system must only allow the opening of which door?
* The external facing door
* The internal facing door
* The last activated door
* The least secure door

Explanation

According to the PCI Card Production and Provisioning Physical Security Requirements, the vendor must have a secure inner shipping delivery room that is equipped with an alarm system and an access-control system. The alarm system must be triggered when any door of the inner shipping delivery room is opened without proper authorization. The access-control system must only allow the opening of the last activated door to liberate a person detected inside of the inner shipping delivery room and stop the alarm. This is to prevent unauthorized access or exit from the inner shipping delivery room, and to ensure that only one door can be opened at a time. References: PCI Card Production and Provisioning Physical Security Requirements and Test Procedures v3.0, January 2022, pages 18-191

Q36. The receptionist responsible for the entrance and departure of visitors must have which of the following?
* A shredder for the destruction of disposable visitor badges
* A constant, open communication channel with a guard
* An unobstructed view of the reception area at all times
* A means of communicating directly with the visitor while on the premises

Explanation

According to the PCI Card Production Physical Security Requirements, the receptionist responsible for the entrance and departure of visitors must have an unobstructed view of the reception area at all times. This is to ensure that the receptionist can monitor and control the access of visitors, and to prevent any unauthorized entry or exit of personnel or materials. The receptionist must also have a means of verifying the identity of visitors, such as a photo ID or a visitor log, and a means of issuing and collecting visitor badges, such as a badge printer or a badge holder. The receptionist must also have a means of communicating with the security personnel or the security control room, such as a phone or an intercom, in case of any emergency or suspicious activity. References:

PCI Card Production Physical Security Requirements, v2.0, April 2019, page 21, requirement 5.3.1 PCI Card Production Physical Security Requirements, v2.0, April 2019, page 22, requirement 5.3.2 PCI Card Production Physical Security Requirements, v2.0, April 2019, page 23, requirement 5.3.3

Q37. After reviewing their completed ROC and AOC, which state that they are compliant, the vendor wishes to be listed on PCI SSC’s list of Compliant Card Vendors. How should you assist them with the listing process?
* Submit the full ROC to PCI SSC
* Submit only the AOC to PCI SSC
* Inform the vendor that PCI SSC does not list compliant vendors
* Inform the vendor that they must request a listing via the payment brand(s) that received their ROC

Explanation

According to the CPSA Program Guide1, PCI SSC does not list compliant card vendors on its website. The PCI SSC only lists the qualified CPSA Companies and CPSA Employees who are authorized to perform PCI Card Production Security Assessments. The PCI SSC also does not receive or review the full ROCs or AOCs from the card vendors or the CPSA Companies. The ROCs and AOCs are submitted by the CPSA Companies to the applicable payment brands that have contracted with the card vendors for card production and provisioning services. The payment brands are responsible for verifying the compliance status of the card vendors and determining whether to list them on their own websites or databases. Therefore, the CPSA Company should inform the vendor that they must request a listing via the payment brand(s) that received their ROC, and that the listing process may vary depending on the payment brand’s policies and procedures.

The CPSA Company should also advise the vendor to maintain their compliance with the PCI Card Production Standards and to undergo annual assessments by a qualified CPSA Company.

Q38. An assessor must provide which of the following to their client at the start of every assessment?
* CPSA Feedback Form

* Quality Assurance Manual
* Attestation of Compliance
* Vendor Release Agreement

Explanation

According to the Card Production Security Assessor (CPSA) Qualification Requirements, an assessor must provide their client with a Quality Assurance Manual at the start of every assessment. The Quality Assurance Manual is a document that describes the assessor’s methodology, procedures, and quality control measures for conducting assessments. The manual must be consistent with the CPSA Program Guide and the PCI Card Production and Provisioning Security Requirements. The manual must also include a description of the assessor’s roles and responsibilities, the assessment scope and objectives, the assessment plan and timeline, the assessment report format and content, and the assessor’s conflict of interestpolicy. References: Card Production Security Assessor (CPSA) Qualification Requirements, v1.0, April 2019, page 111

Q39. Which of the following security awareness measures is required for compliance?

* Annual training on common attack methods
* Annual training on use of mantraps
* Security awareness exams for all personnel
* Security posters must be placed in the facility

Explanation

According to the PCI Card Production and Provisioning Logical Security Requirements, the vendor must implement a formal security awareness program to make all personnel aware of the importance of card production and provisioning security. The security awareness program must include annual training on common attack methods, such as phishing, social engineering, malware, and ransomware, and how to prevent, detect, and report them. The security awareness program must also include training on the vendor’s security policies and procedures, the roles and responsibilities of personnel, the applicable PCI Card Production and Provisioning Security Requirements, and the consequences of non-compliance. The vendor must also require all personnel to acknowledge at least annually that they have read and understood the security policies and procedures. The vendor must not use security posters alone, as they are not sufficient to meet the security awareness program requirements. The vendor may use security awareness exams for all personnel, but they are not mandatory for compliance. The vendor may also train personnel on the use of mantraps, but this is not relevant to the logical security requirements. References: PCI Card Production and Provisioning Logical Security Requirements and Test Procedures v3.0, January 2022, pages 28-291

Q40. A vendor is unsure which forms are needed to complete an assessment. Who should they ask?

* Assessor
* Issuing banks
* Payment brands
* PCI SSC

Explanation

The assessor is the person who conducts the PCI Card Production Security Assessment and prepares the Card Production Report on Compliance (ROC) and the Card Production Attestation of Compliance (AOC). The assessor should be familiar with the forms that are needed to complete an assessment and provide guidance to the vendor on how to fill them out. The assessor should also ensure that the forms are consistent with the PCI Card Production Standards and the PCI CPSA Qualification Requirements. The other options are not the best sources of information for the vendor, as they may not be directly involved in the assessment process or have the expertise to advise on the forms. References:

PCI Card Production Security Assessor (CPSA) Program Guide, Version 1.0, April 2019, page 81 PCI Card Production Security Assessor (CPSA) Qualification Requirements, Version 1.0, April 2019, page 10 PCI Card Production and Provisioning Template for Report on Compliance, Version 1.0, April 2019, page 3 PCI Card Production and Provisioning Attestation of Compliance, Version 1.0, April 2019, page 22

Q41. Which of the following personnel changes must result in the vendor notifying the Vendor Program Administration (VPA)?
* Adding additional rights to someone’s role to give them access to the mam production vault
* Any change to a role that directly affects the security of card products and related components
* Hiring someone that will directly interact with the card issuers
* Promoting someone to senior management level

Explanation

According to the PCI CPSA Qualification Requirements, one of the administrative requirements for CPSA Companies is to notify the VPA of any changes to the roles of CPSA Employees or other personnel that directly affect the security of card products and related components. This is to ensure that the CPSA Company maintains the quality and integrity of the CPSA Program and the PCI Card Production Security Standards. The VPA should be notified within 10 business days of the change, and the CPSA Company should provide evidence of the qualifications and training of theaffected personnel. References: PCI CPSA Qualification Requirements, Version 1.1, April 2020, Section 6.1.3, Page 121

Q42. A vendor has a list of pre-approved third parties which may be granted access to the facility. Under what circumstances can other third-parties be granted access?
* None, only people on the pre-approved list may enter
* When they are approved by the physical security manager or senior management
* When the third party s liability insurance covers the risk
* When no card production activities are taking place

Explanation

According to the PCI Card Production Logical Security Requirements, vendors must have a list of pre-approved third parties that are authorized to access the facility and the systems involved in card production. However, other third parties may be granted access under exceptional circumstances, such as emergency repairs or maintenance, provided that they are approved by the physical security manager or senior management. The vendor must also ensure that the third parties comply with the security policies and procedures, and that their access is logged and monitored. References: PCI Card Production Logical Security Requirements, v2.0, April 2019, page 13

Q43. Which of the following statements is true about the facility’s non-emergency exits?
* They must be contact-alarm monitored only when card production activities are taking place
* They must be configured to prevent staff tailgating
* They may be left unlocked when a guard is present
* They must be fitted with biometric access-control devices

Explanation

According to the PCI Card Production and Provisioning Physical Security Requirements, the vendor must ensure that all non-emergency exits are configured to prevent staff tailgating. Tailgating is the act of following someone closely through a door or other entry point without proper authorization. The vendor must use access-control devices, such as turnstiles, mantraps, or biometric readers, to prevent tailgating and unauthorized access or exit. The vendor must also monitor and alarm all non-emergency exits 24/7, and have procedures to respond to any alarms or incidents. The vendor must not leave any non-emergency exits unlocked, even when a guard is present, as this may compromise the security of the facility and the card production andprovisioning materials. References: PCI Card Production and Provisioning Physical Security Requirements and Test Procedures v3.0, January 2022, pages 8-91

Q44. During an assessment you ask to see employee records for employees with access to the HSA. The records include information about the screening process, including background information from the employee application process. The oldest background Information that is available is for an employee that left the vendor (terminated their contract) one year previously. You note this as non-compliant, why?

* Employee information, including background checks, must be stored for at least seven years
* Employee information must be securely destroyed (e.g. securely wiped) within 2 years (after termination of contract)
* The vendor must retain the background information for at least 18 months after termination of contract
* The vendor must only retain background information for all current employees, not for those that have been terminated

Explanation

According to the PCI Card Production Logical Security Requirements, the vendor must securely destroy all employee information, including background checks, within two years of the employee’s termination of contract. This is to prevent unauthorized access to sensitive employee data and to comply with the PCI DSS requirement 3.1, which states that cardholder data must not be stored longer than necessary. The vendor must also have a documented policy and procedure for the secure destruction of employee information, and must maintain a log of all destruction activities. References:

PCI Card Production Logical Security Requirements, v2.0, April 2019, page 19, requirement 6.1.1 PCI DSS, v3.2.1, May 2018, page 25, requirement 3.1

Q45. How frequently must alarms on external doors of a card production and provisioning vendor environment be tested?
* Every day
* Every week
* Every month
* Every 3 months

Explanation

According to the PCI Card Production and Provisioning Physical Security Requirements, the vendor must test all alarms on external doors of the card production and provisioning vendor environment at least every month.

The vendor must also document the results of the tests and retain them for at least one year. The vendor must also have procedures to respond to any alarms or incidents, and to report them to the relevant parties. The vendor must not test the alarms less frequently than every month, as this may compromise the security and integrity of the card production and provisioning vendor environment and increase the risk of unauthorized access or theft. References: PCI Card Production and Provisioning Physical Security Requirements and Test Procedures v3.0, January 2022, pages 9-101

Q46. If a vendor plans to terminate an employee, which of these must be done?
* The employee must be escorted from the premises immediately
* The employee’s locker and desk must be searched prior to termination
* The Human Resources department must be notified prior to termination
* The security manager must be notified in writing prior to termination

Explanation

According to the PCI Card Production Logical Security Requirements, the vendor must have a formal employee termination process that includes notifying the security manager in writing prior to the termination of any employee who has access to cardholder data or sensitive authentication data. This is to ensure that the security manager can take appropriate actions to revoke the employee’s access rights, credentials, and keys, and to prevent any unauthorized use or disclosure of cardholder data or sensitive authentication data by the terminated employee. The vendor must also have a documented policy and procedure for the employee termination process, and must maintain a log of all termination activities. References:

PCI Card Production Logical Security Requirements, v2.0, April 2019, page 19, requirement 6.1.2 PCI Card Production Logical Security Requirements, v2.0, April 2019, page 20, requirement 6.1.3

Q47. John works for ACME Inc Personalizers. an organization that personalizes payment cards as well as printing the corresponding PIN mailers for distribution directly to the cardholder. Which of the following statements is true?

* If John is involved in card personalization then he must not be involved in the printing of the corresponding PINs
* If John is involved in card personalization, then he must never be involved in the card shipment process
* If John is involved in card personalization, then he must never be involved in PIN printing
* If John is involved in PIN printing, then he must never be involved in the card shipment process

Explanation

According to the PCI Card Production and Provisioning – Logical Security Requirements, there must be a clear segregation of duties between the staff involved in different card production and provisioning activities, such as card personalization, PIN generation and printing, and card fulfillment. This is to prevent any unauthorized access, modification, or disclosure of sensitive cardholder data and to ensure the integrity and confidentiality of the card production process. Therefore, if John is involved in card personalization, which is the process of transferring cardholder information to a payment card, then he must never be involved in PIN printing, which is the process of printing the personal identification number associated with the cardholder account on a mailer. This way, John cannot link the cardholder data on the card with the PIN on the mailer, and cannot compromise the security of the cardholder authentication. The other statements are not true, as there is no requirement that prohibits John from being involved in the card shipment process, as long as he does not have access to both the card and the PIN mailer at the same time. References:

Payment Card Industry (PCI) Card Production and Provisioning – Logical Security Requirements, Section 2.1.1 and 2.1.2
Payment Card Industry (PCI) Card Production and Provisioning – Glossary of Terms, Abbreviations, and Acronyms, Definitions of Card Personalization and PIN Printing

Q48. A vendor is unsure which forms are needed to complete an assessment. Who should they ask?
* Payment brands
* Issuing banks
* PCI SSC
* Assessor

Q49. Which of the following statements about unsolicited visitors is true?
* They must be turned away
* They must complete an NDA before entry is granted
* They must be able to prove a legitimate reason for their visit prior to entry
* They must be registered, their identities confirmed, and must be allocated an escort before entry

Explanation

According to the PCI Card Production and Provisioning Physical Security Requirements, unsolicited visitors are defined as “individuals who do not have a pre-arranged appointment or a legitimate reason for visiting the Card Production Entity”. The requirement for dealing with unsolicited visitors is that they must be registered, their identities confirmed, and must be allocated an escort before entry. The escort must accompany the unsolicited visitor at all times and ensure that they do not access any restricted areas or sensitive information.

The other options are not true statements about unsolicited visitors, as they may not comply with the PCI Card Production Standards or the best practices for physical security. References:

PCI Card Production and Provisioning Physical Security Requirements, Version 1.0, April 2019, page

101

PCI Card Production and Provisioning Physical Security Requirements, Version 1.0, April 2019, page

111

Prepare For Realistic CPSA_P_New Dumps PDF - 100% Passing Guarantee:
https://www.examcollectionpass.com/PCI/CPSA_P_New-practice-exam-dumps.html]