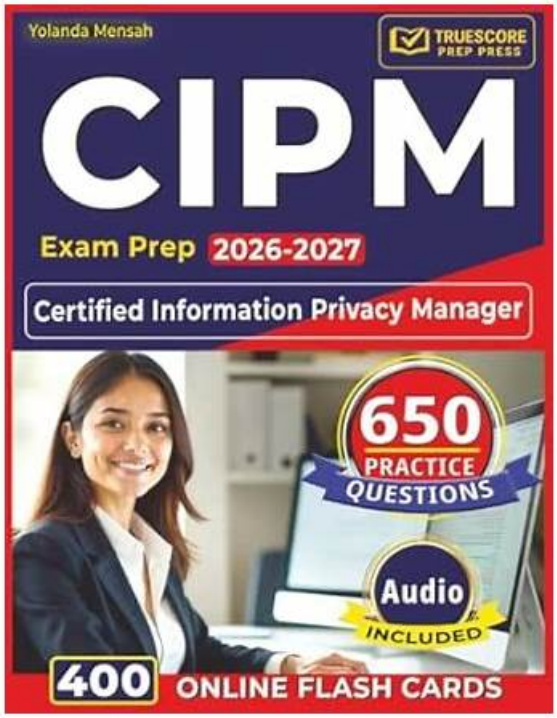
Certified Information Privacy Manager (CIPM) Exam Practice Dump Provide Best CIPM Study Questions



DOWNLOAD the newest BraindumpsVCE CIPM PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=185Jvrph2GVrkl9vs14kESnGN-BtnL252

As we all know, the latest CIPM quiz prep has been widely spread since we entered into a new computer era. The cruelty of the competition reflects that those who are ambitious to keep a foothold in the job market desire to get the CIPM certification. As long as you spare one or two hours a day to study with our laTest CIPM Quiz prep, we assure that you will have a good command of the relevant knowledge before taking the exam. What you need to do is to follow the CIPM exam guide system at the pace you prefer as well as keep learning step by step.

The International Association of Privacy Professionals (IAPP) CIPM (Certified Information Privacy Manager) exam is a rigorous certification exam that assesses the knowledge and skills of individuals who manage privacy programs. CIPM exam is designed to test the knowledge and understanding of privacy laws and regulations, privacy program management, privacy operations, and communication and training. Passing the CIPM exam is a testament to an individual's knowledge and experience in managing privacy programs.

The International Association of Privacy Professionals (IAPP) Certified Information Privacy Manager (CIPM) Certification Exam is a globally recognized certification program designed for professionals who are responsible for managing and overseeing privacy programs within their organizations. CIPM Exam is intended to test the knowledge and skills of candidates in the area of privacy management and provide them with a credential that demonstrates their expertise in privacy management.

>> Frequent CIPM Updates <<

Reliable CIPM Exam Simulator - CIPM Actual Exam

The IAPP CIPM exam questions formats are PDF dumps files, desktop practice test software, and web-based practice test software. All these CIPM exam questions format hold some common and unique features. Such as CIPM PDF dumps file is the PDF version of Prepare for your IAPP CIPM Exam Dumps that works with all operating systems and devices. Whereas the other two CIPM practice test questions formats are concerned, both are the mock IAPP CIPM exam.

The CIPM Certification demonstrates a professional's commitment to privacy management and their ability to navigate the complex and ever-changing privacy landscape. Certified Information Privacy Manager (CIPM) certification is accredited by the American National Standards Institute (ANSI) and is recognized by privacy regulators and organizations around the world. Certified Information Privacy Manager (CIPM) certification exam is based on the International Association of Privacy Professionals (IAPP) Privacy Program Management: Tools for Managing Privacy Within Your Organization textbook, which is a comprehensive guide to developing, implementing, and managing a privacy program.

IAPP Certified Information Privacy Manager (CIPM) Sample Questions (Q240-Q245):

NEW QUESTION # 240
Which of the following practices best ensures the continuous assessment of program performance within the operational life cycle?

- A. Evaluating emerging risks every 24 months.
- B. Allocating training costs in favor of the privacy and security teams.
- C. Prioritizing ongoing improvement efforts.
- D. Completing third-party audits by subject matter experts.

Answer: C

Explanation:
Continuous assessment requires ongoing improvement embedded into operations. Periodic audits or infrequent evaluations do not provide real-time insight. CIPM promotes continuous improvement as a maturity driver.

NEW QUESTION # 241
SCENARIO
Please use the following to answer the next QUESTION:
It's just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It's a great deal, and after a month, more than half the organization's employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them, potentially carrying personal data to their homes or other unknown locations. It's enough to give you data- protection nightmares, and you've pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.
Today you have in your office a representative of the organization's marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop "safely" tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.
You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.
From a business standpoint, what is the most productive way to view employee use of personal equipment for work-related tasks?

- A. The use of personal equipment must be reduced as it leads to inevitable security risks.
- B. The use of personal equipment is a cost-effective measure that leads to no greater security risks than are always present in a modern organization.
- C. While the company may not own the equipment, it is required to protect the business-related data on any equipment used

by its employees.

- D. Any computer or other equipment is company property whenever it is used for company business.

Answer: C

Explanation:
Explanation
This answer reflects the principle of accountability, which states that the company is responsible for ensuring that personal data is processed in compliance with applicable laws and regulations, regardless of who owns or controls the equipment that stores or processes the data. The company should establish policies and procedures for managing the use of personal equipment for work-related tasks, such as requiring encryption, authentication, remote wipe, backup and reporting of incidents. The company should also provide training and awareness to the employees on how to protect the data on their personal equipment and what are their obligations and liabilities. References: IAPP CIPM Study Guide, page 841; ISO/IEC 27002:2013, section
6.2.1

NEW QUESTION # 242
SCENARIO
Please use the following to answer the next QUESTION:
Martin Briseno is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseno decided to change the hotel's on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading Briseno to work with corporate HR specialists and software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.
Upon hearing about the success of Briseno's program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online.
As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.
By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the user's name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and 2008, PHT issued more than 700,000 professional certifications.
PHT's profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e- learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved. The training program's systems and records remained in Pacific Suites' digital archives, un- accessed and unused. Briseno and Silva-Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They planned to deal with the PHT materials once resources allowed.
In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific Hospitality Training's customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.
A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.
PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity.
In the Information Technology engineers had originally set the default for customer credit card information to "Do Not Save," this action would have been in line with what concept?

- A. Privacy by Design
- B. Harm minimization

- C. Reactive risk management
- D. Use limitation

Answer: A

NEW QUESTION # 243
Please use the following to answer the next QUESTION:
You lead the privacy office for a company that handles information from individuals living in several countries throughout Europe and the Americas. You begin that morning's privacy review when a contracts officer sends you a message asking for a phone call. The message lacks clarity and detail, but you presume that data was lost.
When you contact the contracts officer, he tells you that he received a letter in the mail from a vendor stating that the vendor improperly shared information about your customers. He called the vendor and confirmed that your company recently surveyed exactly 2000 individuals about their most recent healthcare experience and sent those surveys to the vendor to transcribe it into a database, but the vendor forgot to encrypt the database as promised in the contract. As a result, the vendor has lost control of the data.
The vendor is extremely apologetic and offers to take responsibility for sending out the notifications. They tell you they set aside 2000 stamped postcards because that should reduce the time it takes to get the notice in the mail. One side is limited to their logo, but the other side is blank and they will accept whatever you want to write. You put their offer on hold and begin to develop the text around the space constraints. You are content to let the vendor's logo be associated with the notification.
The notification explains that your company recently hired a vendor to store information about their most recent experience at St. Sebastian Hospital's Clinic for Infectious Diseases. The vendor did not encrypt the information and no longer has control of it. All 2000 affected individuals are invited to sign-up for email notifications about their information. They simply need to go to your company's website and watch a quick advertisement, then provide their name, email address, and month and year of birth.
You email the incident-response council for their buy-in before 9 a.m. If anything goes wrong in this situation, you want to diffuse the blame across your colleagues. Over the next eight hours, everyone emails their comments back and forth. The consultant who leads the incident-response team notes that it is his first day with the company, but he has been in other industries for 45 years and will do his best. One of the three lawyers on the council causes the conversation to veer off course, but it eventually gets back on track. At the end of the day, they vote to proceed with the notification you wrote and use the vendor's postcards.
Shortly after the vendor mails the postcards, you learn the data was on a server that was stolen, and make the decision to have your company offer credit monitoring services. A quick internet search finds a credit monitoring company with a convincing name: Credit Under Lock and Key (CRUDLOK). Your sales rep has never handled a contract for 2000 people, but develops a proposal in about a day which says CRUDLOK will:
1.Send an enrollment invitation to everyone the day after the contract is signed.
2.Enroll someone with just their first name and the last-4 of their national identifier.
3.Monitor each enrollee's credit for two years from the date of enrollment.
4.Send a monthly email with their credit rating and offers for credit-related services at market rates.
5.Charge your company 20% of the cost of any credit restoration.
You execute the contract and the enrollment invitations are emailed to the 2000 individuals. Three days later you sit down and document all that went well and all that could have gone better. You put it in a file to reference the next time an incident occurs.
Regarding the credit monitoring, which of the following would be the greatest concern?

- A. The vendor's representative does not have enough experience
- B. The company did not collect enough identifiers to monitor one's credit
- C. You are going to notify affected individuals via a letter followed by an email
- D. Signing a contract with CRUDLOK which lasts longer than one year

Answer: B

Explanation:
Explanation
This answer is the greatest concern regarding the credit monitoring, as it may compromise the accuracy and effectiveness of the service, as well as expose the affected individuals to further privacy and security risks. The company did not collect enough identifiers to monitor one's credit means that the company only asked for the first name and the last-4 of their national identifier from the enrollees, which may not be sufficient or unique to identify and verify their identity and credit history. This may lead to errors, disputes or inaccuracies in the credit monitoring service, as well as potential identity theft, fraud or misuse of the data by unauthorized or malicious parties.

NEW QUESTION # 244

What is the main function of the Asia-Pacific Economic Cooperation Privacy Framework?

- A. Marketing privacy protection technologies developed in the region
- B. Protecting data from parties outside the region
- C. Establishing legal requirements for privacy protection in the region
- D. Enabling regional data transfers

Answer: D

NEW QUESTION # 245

.....