

100% Pass Quiz 2026 Latest CIPM: Cert Certified Information Privacy Manager (CIPM) Exam



BTW, DOWNLOAD part of Exam4Tests CIPM dumps from Cloud Storage: https://drive.google.com/open?id=1Pkd4TCWLOPaahp1c0QL0f_5Cjq8QJXfG

The IAPP CIPM certification exam is without a doubt a terrific and quick way to develop your profession in your field. These advantages include the opportunity to develop new, in-demand skills, advantages in the marketplace, professional credibility, and the opening up of new job opportunities. Certified Information Privacy Manager (CIPM) CIPM real reliable test cram and test book help you pass the Certified Information Privacy Manager (CIPM) exam successfully.

The CIPM exam covers a broad range of topics related to privacy management, including privacy program governance, privacy program operationalization, privacy program assessment, and privacy program communication. CIPM exam also covers the legal and regulatory frameworks related to privacy, such as GDPR, CCPA, and HIPAA. The CIPM Exam is designed for professionals with at least two years of experience in privacy management or a related field. CIPM exam consists of 90 multiple-choice questions and must be completed within two hours.

>> Cert CIPM Exam <<

2026 Cert CIPM Exam | Efficient 100% Free Free CIPM Vce Dumps

Our company is a professional certification exam materials provider, we have occupied in the field more than ten years, and we have rich experiences. CIPM training materials have gained popularity in the international market for high quality. In addition, CIPM exam, dumps contain both questions and answers, and you can have a quick check after practicing. CIPM Training Materials cover most of knowledge points for the exam, and they will help you pass the exam. We offer you free update for 365 days after purchasing CIPM exam materials, and the update version will be sent to your email automatically.

IAPP Certified Information Privacy Manager (CIPM) Sample Questions (Q23-Q28):

NEW QUESTION # 23
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, unaccessed 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.

What must Pacific Suite's primary focus be as it manages this security breach?

- A. Maintaining operations and preventing publicity
- **B. Minimizing the amount of harm to the affected individuals**
- C. Determining whether the affected individuals should be notified
- D. Investigating the cause and assigning responsibility

Answer: B

NEW QUESTION # 24

Which of the following indicates you have developed the right privacy framework for your organization?

- A. It works at a different type of organization.
- **B. It improves the consistency of the privacy program.**
- C. It identifies all key stakeholders by name.
- D. It includes a privacy assessment of each major system.

Answer: B

Explanation:

Explanation

Developing the right privacy framework for your organization means that you have a clear and coherent set of policies, procedures,

and practices that align with your privacy objectives and obligations. A good privacy framework should improve the consistency of the privacy program by ensuring that all relevant stakeholders understand and follow the same standards and expectations across different functions, processes, and systems.

A consistent privacy program can also help reduce errors, risks, and costs associated with privacy compliance.

NEW QUESTION # 25

A systems audit uncovered a shared drive folder containing sensitive employee data with no access controls and therefore was available for all employees to view. What is the first step to mitigate further risks?

- A. Notify all employees whose information was contained in the file.
- **B. Restrict access to the folder.**
- C. Check access logs to see who accessed the folder.
- D. Notify legal counsel of a privacy incident.

Answer: B

Explanation:

Explanation

The first step to mitigate further risks when a systems audit uncovers a shared drive folder containing sensitive employee data with no access controls is to restrict access to the folder. This can be done by implementing appropriate access controls, such as user authentication, role-based access, and permissions, to ensure that only authorized individuals can view and access the sensitive data.

NEW QUESTION # 26

Under which circumstances would people who work in human resources be considered a secondary audience for privacy metrics?

- A. They do not receive training on privacy issues
- **B. They do not have privacy policy as their main task**
- C. They do not interface with the financial office
- D. They do not have frequent interactions with the public

Answer: B

Explanation:

People who work in human resources would be considered a secondary audience for privacy metrics if they do not have privacy policy as their main task. A secondary audience is a group of stakeholders who are indirectly involved or affected by the privacy program, but do not have primary responsibility or authority over it. They may use privacy metrics to support their own functions or objectives, such as hiring, training, or compliance. Reference: IAPP CIPM Study Guide, page 23.

NEW QUESTION # 27

SCENARIO

Please use the following to answer the next QUESTION:

As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company.

In fact, you consider your program a model that others in the data storage industry may note in their own program development.

You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.

Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.

Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.

You are left contemplating:

