

CIPM Free Exam Questions, CIPM Study Group



Examples of CIPM Principles Exam Questions

Based upon actual exam questions, these examples are intended to help you decide whether to become a candidate for the CIPM designation. They display the format of the multiple choice questions that appear on the Principles exam, and they illustrate some of the concepts on which Principles candidates have been tested in the past. The questions are grouped into three major topic areas: ethical and professional standards, performance evaluation, and the GIPS standards. An answer key is provided at the end of this document.

Topic Area: Ethical and Professional Standards

1. Which of the following practices is *most likely* to violate the fair dealing provision of the CIPM Association Standards of Professional Conduct?
 - A. Trading for the firm's account prior to allowing employees to trade for their own accounts.
 - B. Selling a security from taxable accounts prior to selling the same security from tax-exempt accounts.
 - C. Offering insurance companies specialized portfolio accounting services without informing pension funds that such services are available.
2. Information is *most accurately* described as *nonpublic* if it:
 - A. pertains to a company's future per-share earnings.
 - B. would be taken into account by a reasonable investor.
 - C. has been disclosed to relatively few market participants.
3. When writing a research report, Dennis Donaldson, CIPM, consults another investment analyst's published report on the same topic. Donaldson does not acknowledge the other analyst's original work. Donaldson is *least likely* to violate the CIPM Association Standards of Professional Conduct if he:
 - A. considers the other analyst's work in reaching his own conclusions.
 - B. reproduces the other analyst's factual data but reaches his own conclusions.
 - C. independently confirms the other analyst's facts and rephrases her conclusions.

Topic Area: Performance Evaluation

4. Matthew O'Reilly invests €2,000 in a mutual fund at the beginning of the year. The mutual fund has a positive return for the first six months and a negative return for the second six months of the year. The money-weighted return of the O'Reilly account for the year is *most likely* to be:
 - A. lower than its time-weighted return.
 - B. the same as its time-weighted return.
 - C. higher than its time-weighted return.

© 2009 CFA Institute

Examples of CIPM Principles Exam Questions, p. 1 of 5

BTW, DOWNLOAD part of PracticeVCE CIPM dumps from Cloud Storage: https://drive.google.com/open?id=18pbh-CSQvDmxF_p7hjQxKAgQ3PPLC1Tu

Experts have prepared the CIPM desktop-based exam simulation software. There are CIPM actual questions in the practice test to give you an exact impression of the Certified Information Privacy Manager (CIPM) CIPM original test. This type of Certified Information Privacy Manager (CIPM) CIPM actual exam simulations helps to calm your anxiety.

The CIPM certification is an excellent choice for privacy professionals who are looking to enhance their knowledge and skills in privacy management, demonstrate their expertise to employers and clients, and gain a competitive advantage in the job market. With the growing importance of data protection and privacy regulations, the demand for privacy professionals is only expected to increase, making the CIPM certification even more valuable in the years to come.

The CIPM exam is designed to test your knowledge and expertise in privacy management. It is a rigorous exam that requires a comprehensive understanding of privacy laws, regulations, standards, and best practices. CIPM exam is divided into two parts: Part 1 consists of 80 multiple-choice questions, and Part 2 is a scenario-based exam with 35 multiple-choice questions.

The CIPM Exam covers a wide range of privacy-related topics, including data protection regulations, data governance, risk management, and privacy program management. CIPM exam is designed to assess the candidate's ability to apply privacy principles and best practices in the workplace, as well as their understanding of the legal and regulatory frameworks that govern data protection. CIPM exam also tests the candidate's ability to develop and implement effective privacy policies and procedures that are in line with industry standards and best practices.

>> CIPM Free Exam Questions <<

Certified Information Privacy Manager (CIPM) practice dumps & CIPM exam dumps

PracticeVCE guarantee the most valid and high quality CIPM study guide which you won't find any better one available. Our CIPM training pdf will be the right study reference if you want to be 100% sure pass and get satisfying results. From our free demo which allows you free download, you can see the validity of the questions and format of the CIPM Actual Test. In addition, the price of our CIPM examination material is reasonable and affordable for all of you. Just come and buy our CIPM training questions!

IAPP Certified Information Privacy Manager (CIPM) Sample Questions (Q20-Q25):

NEW QUESTION # 20

Formosa International operates in 20 different countries including the United States and France.

What organizational approach would make complying with a number of different regulations easier?

- A. Rationalizing requirements.
- B. Decentralized privacy management.
- C. Fair Information Practices.
- D. Data mapping.

Answer: C

NEW QUESTION # 21

SCENARIO

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

Answer: D

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 # 22

If your organization has a recurring issue with colleagues not reporting personal data breaches, all of the following are advisable to do EXCEPT?

- A. Provide role-specific training to areas where breaches are happening so they are more aware.
- B. Improve communication to reinforce to everyone that breaches must be reported and how they should be reported.
- C. Review reporting activity on breaches to understand when incidents are being reported and when they are not to improve communication and training.
- **D. Distribute a phishing exercise to all employees to test their ability to recognize a threat attempt.**

Answer: D

Explanation:

Distributing a phishing exercise is not advisable when attempting to address the issue of colleagues not reporting personal data breaches. Instead, the recommended steps are to review reporting activity on breaches, improve communication, and provide role-specific training to areas where breaches are happening. These steps will help to ensure that everyone is aware of their responsibilities and that they understand how to report a breach should one occur.

Reference:

<https://www.itgovernance.co.uk/blog/5-reasons-why-employees-dont-report-data-breaches/>

<https://www.ncsc.gov.uk/guidance/report-cyber-incident>

<https://www.ncsc.gov.uk/guidance/phishing-staff-awareness>

NEW QUESTION # 23

SCENARIO

Please use the following to answer the next QUESTION:

Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.

Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the "misunderstanding" has not occurred again.

As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.

Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. "The good news," he says, "is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud." Lately, you have been hearing about cloud computing and you know it's fast becoming the new paradigm for various applications. However, you have heard mixed reviews about the potential impacts on privacy protection. You begin to research and discover that a number of the leading cloud service providers have signed a letter of intent to work together on shared conventions

and technologies for privacy protection. You make a note to find out if Jason's Finnish provider is signing on. What is the best way for your vendor to be clear about the Society's breach notification expectations?

- A. Email the regulations that require breach notifications
- **B. Include notification provisions in the vendor contract**
- C. Send a memorandum of understanding on breach notification
- D. Arrange regular telephone check-ins reviewing expectations

Answer: B

Explanation:

Explanation

This answer is the best way for Albert's vendor to be clear about the Society's breach notification expectations, as it can establish clear and binding terms and conditions for both parties regarding their roles and responsibilities for handling any data security incidents or breaches. Including notification provisions in the vendor contract can help to define what constitutes a breach, how it should be detected, reported and investigated, what information should be provided to the organization and within what time frame, what actions should be taken to mitigate or resolve the breach, and what consequences or liabilities may arise from the breach. The contract can also specify that the vendor must cooperate and coordinate with the organization in any breach notification activities to the relevant authorities, customers, partners or stakeholders.

NEW QUESTION # 24

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.

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

- Answer: C**

• • • • •

BTW, DOWNLOAD part of PracticeVCE CIPM dumps from Cloud Storage: https://drive.google.com/open?id=18pbh-CSQvDmxF_p7hjQxKAqQ3PPLC1Tu