CIPM Q&As

Certified Information Privacy Manager

Pass IAPP CIPM Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/cipm.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What should be the first major goal of a company developing a new privacy program?

A. To survey potential funding sources for privacy team resources.

B. To schedule conversations with executives of affected departments.

C. To identify potential third-party processors of the organization\\'s information.

D. To create Data Lifecycle Management policies and procedures to limit data collection.

Correct Answer: D

QUESTION 2

SCENARIO

Please use the following to answer the next question:

Jonathan recently joined a healthcare payment processing solutions company as a senior privacy manager. One morning, Jonathan awakens to several emails informing him that an individual cloud server failed due to a flood in its server

room, damaging its hardware and destroying all the data the company had stored on that drive. Jonathan was not aware that the company had this particular cloud account or that any data was being stored there because it was not included

in the data mapping or data inventory provided to him by his predecessor. Jonathan\\'s predecessor conducted a data inventory and mapping exercise 4 years ago and updated it on an annual basis.

Renee works in the sales department and tells Jonathan that she doesn\\'t think that account had been used since the company moved to a bigger cloud vendor three years ago. She also advised him that the account was mostly used by

Human Resources (HR) and Accounts Payable (AP). Jonathan speaks to both departments and learns that each had met with his predecessor multiple times and explained they saved sensitive personal data on that drive, including health

and financial related personal data and "other stuff." Jonathan also learns that the data stored in that account was not backed up pursuant to company policy. Jonathan asks his IT department who had access to that particular account and

learns that there were no access controls in place, making the account available to anyone in the company, despite the purported sensitivity of the data being stored there.

Jonathan is panicking as the data can\\'t be recovered, and he can\\'t determine exactly what data was saved on that account or to whom it belongs. Two days later, the company receives 32 data subject access requests and Accounts Payable

confirms Jonathan\\'s worry that these data subjects\\' personal data was likely stored on this account. He searches for the company\\'s data subject access request policy, but later learns it doesn\\'t exist.

Jonathan wants to formalize monitoring to prevent a similar issue from happening again. What scope of monitoring would be most useful?

A. Monitoring compliance with data mapping and disaster recovery.

B. Monitoring new privacy legislation and industry standards for information security.

C. Monitoring the vulnerabilities across environments containing sensitive personal data.

D. Monitoring of vendor contracts to ensure security controls are systematically addressed.

Correct Answer: C

QUESTION 3

SCENARIO Please use the following to answer the next QUESTION: Natalia, CFO of the Nationwide Grill restaurant chain, had never seen her fellow executives so anxious. Last week, a data processing firm used by the company reported that its system may have been hacked, and customer data such as

names, addresses, and birthdays may have been compromised. Although the attempt was proven unsuccessful, the scare has prompted several Nationwide Grill executives to Question the company\\'s privacy program at today\\'s meeting.

Alice, a vice president, said that the incident could have opened the door to lawsuits, potentially damaging Nationwide Grill\\'s market position. The Chief Information Officer (CIO), Brendan, tried to assure her that even if there had been an actual breach, the chances of a successful suit against the company were slim. But Alice remained unconvinced. Spencer ?a former CEO and currently a senior advisor ?said that he had always warned against the use of contractors for data processing. At the very least, he argued, they should be held contractually liable for telling customers about any security incidents. In his view, Nationwide Grill should not be forced to soil the company name for a problem it did not cause. One of the business development (BD) executives, Haley, then spoke, imploring everyone to see reason. "Breaches can happen, despite organizations\\' best efforts," she remarked. "Reasonable preparedness is key." She reminded everyone

of the incident seven years ago when the large grocery chain Tinkerton\\'s had its financial information compromised after a large order of Nationwide Grill frozen dinners. As a long-time BD executive with a solid understanding of Tinkerton\\'s\\'s

corporate culture, built up through many years of cultivating relationships, Haley was able to successfully manage the company\\'s incident response.

Spencer replied that acting with reason means allowing security to be handled by the security functions within the company ?not BD staff. In a similar way, he said, Human Resources (HR) needs to do a better job training employees to

prevent incidents. He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company\\'s privacy program. Both the volume and the duplication of

information means that it is often ignored altogether.

Spencer said, "The company needs to dedicate itself to its privacy program and set regular in-person trainings for all staff once a month."

Alice responded that the suggestion, while well-meaning, is not practical. With many locations, local HR departments need to have flexibility with their training schedules.

Silently, Natalia agreed.

How could the objection to Spencer\\'s training suggestion be addressed?

A. By requiring training only on an as-needed basis.

B. By offering alternative delivery methods for trainings.

C. By introducing a system of periodic refresher trainings.

D. By customizing training based on length of employee tenure.

Correct Answer: B

QUESTION 4

Under the General Data Protection Regulation (GDPR), what obligation does a data controller or processor have after appointing a Data Protection Officer (DPO)?

A. To submit for approval to the DPO a code of conduct to govern organizational practices and demonstrate compliance with data protection principles.

B. To provide resources necessary to carry out the defined tasks of the DPO and to maintain their expert knowledge.

C. To ensure that the DPO acts as the sole point of contact for individuals' questions about their personal data.

D. To ensure that the DPO receives sufficient instructions regarding the exercise of their defined tasks.

Correct Answer: B

QUESTION 5

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.

After conducting research, you discover a primary data protection issue with cloud computing. Which of the following should be your biggest concern?

A. An open programming model that results in easy access

B. An unwillingness of cloud providers to provide security information

C. A lack of vendors in the cloud computing market

D. A reduced resilience of data structures that may lead to data loss.

Correct Answer: B