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.pass4itsure.com/cipm.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

A. Review reporting activity on breaches to understand when incidents are being reported and when they are not to improve communication and training.

B. Improve communication to reinforce to everyone that breaches must be reported and how they should be reported.

C. Provide role-specific training to areas where breaches are happening so they are more aware.

D. Distribute a phishing exercise to all employees to test their ability to recognize a threat attempt.

Correct 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.

References: 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

QUESTION 2

SCENARIO

Please use the following to answer the next question:

You were recently hired by InStyle Data Corp. as a privacy manager to help InStyle Data Corp. became compliant with a new data protection law.

The law mandates that businesses have reasonable and appropriate security measures in place to protect personal data. Violations of that mandate are heavily fined and the legislators have stated that they will aggressively pursue

companies that don\\'t comply with the new law.

You are paired with a security manager and tasked with reviewing InStyle Data Corp.\\'s current state and advising the business how it can meet the “reasonable and appropriate security’ requirement. InStyle Data Corp has grown rapidly and

has not kept a data inventory or completed a data mapping. InStyle Data Corp. has also developed security-related policies ad hoc and many have never been implemented. The various teams involved in the creation and testing of InStyle

Data Corp.\\'s products experience significant turnover and do not have well defined roles. There\\'s little documentation addressing what personal data is processed by which product and for what purpose.

Work needs to begin on this project immediately so that InStyle Data Corp. can become compliant by the time the law goes into effect. You and your partner discover that InStyle Data Corp. regularly sends files containing sensitive personal

data back to its customers, through email, sometimes using InStyle Data Corp employees personal email accounts. You also learn that InStyle Data Corp.\\'s privacy and information security teams are not informed of new personal data flows,

new products developed by InStyle Data Corp. that process personal data, or updates to existing InStyle Data Corp. products that may change what or how the personal data is processed until after the product or update has gone live.

Through a review of InStyle Data Corp' test and development environment logs, you discover InStyle Data Corp. sometimes gives login credentials to any InStyle Data Corp. employee or contractor who requests them. The test environment

only contains dummy data, but the development environment contains personal data, including Social Security Numbers, health information, and financial information. All credentialed InStyle Data Corp. employees and contractors have the

ability to alter and delete personal data in both environments regardless of their role or what project they are working on.

You and your partner provide a gap assessment citing the issues you spotted, along with recommended remedial actions and a method to measure implementation. InStyle Data Corp. implements all of the recommended security controls.

You review the processes, roles, controls, and measures taken to appropriately protect the personal data at every step. However, you realize there is no plan for monitoring and nothing in place addressing sanctions for violations of the

updated policies and procedures. InStyle Data Corp. pushes back, stating they do not have the resources for such monitoring.

In order to mitigate the risk of new data flows, products, or updates that cause InStyle Data Corp. to be noncompliant with the new law you should establish?

A. A process whereby privacy and security would be consulted right before the do-live date for the new data flows, products, or updates.

B. Best practices that require employees to sign an attestation that they understand the sensitivity of new data flows, products, or updates.

C. Access controls based on need-to-know basis for InStyle Data Corp. employees so that not everyone has access to personal data in data flows, products, or updates.

D. Requirements for a Privacy Impact Assessment (PIA) / Data Privacy Impact Assessment (DPIA) as part of the business' standard process in developing new data flows, products, or updates.

Correct Answer: D

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.

The senior advisor, Spencer, has a misconception regarding?

A. The amount of responsibility that a data controller retains.

B. The appropriate role of an organization\\'s security department.

C. The degree to which training can lessen the number of security incidents.

D. The role of Human Resources employees in an organization\\'s privacy program.

Correct Answer: C

QUESTION 4

Which privacy principles and guidelines helped form the basis for the EU Data Protection Directive and The General Data Protection Regulation (GDPR)?

A. Canadian Standards Association Privacy Code (CSA).

B. The European Telecommunications Standards Institute (ETSI).

C. The Asia Pacific Economic Cooperation Privacy Framework (APEC).

D. The Organization for Economic Cooperation and Development (OECD).

Correct Answer: D

QUESTION 5

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:

What must be done to maintain the program and develop it beyond just a data breach prevention program? How can you build on your success?

What are the next action steps?

What process could most effectively be used to add privacy protections to a new, comprehensive program being developed at Consolidated?

A. Privacy by Design.

B. Privacy Step Assessment.

C. Information Security Planning.

D. Innovation Privacy Standards.

Correct Answer: C