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.passapply.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

Training and awareness metrics in a privacy program are necessary to?

A. Identify data breaches.

B. Implement privacy policies.

C. Demonstrate compliance with regulations.

D. Educate customers on the organization\\'s data practices.

Correct Answer: D

QUESTION 2

Which item below best represents how a Privacy Group can effectively communicate with functional areas?

A. Rely solely on items from work units for constructing an impact assessment.

B. Work closely with functional areas by acting as both an advisor and advocate.

C. Focus attention on Directors and Senior Managers as they are responsible for the work.

D. Choose a work unit representative and funnel all communications through that one person.

Correct Answer: B

QUESTION 3

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.

What is the most concerning limitation of the incident-response council?

A. You convened it to diffuse blame

B. The council has an overabundance of attorneys

C. It takes eight hours of emails to come to a decision

D. The leader just joined the company as a consultant

Correct Answer: A

QUESTION 4

Which of the following is a common disadvantage of a third-party audit?

A. It identifies weaknesses of internal controls.

B. It lends credibility to an internal audit program.

C. It requires a learning curve about the organization.

D. It provides a level of unbiased, expert recommendations.

Correct Answer: A

QUESTION 5

You would like to better understand how your organization can demonstrate compliance with international privacy standards and identify gaps for remediation. What steps could you take to achieve this objective?

A. Carry out a second-party audit.

B. Consult your local privacy regulator.

C. Conduct an annual self assessment.

D. Engage a third-party to conduct an audit.

Correct Answer: D

Explanation: Engaging a third-party to conduct an audit is the best way to ensure that your organization is compliant with international privacy standards and identify any gaps that need to be remediated. An audit should include a review of your organization\\'s data processing activities, as well as its policies, procedures, and internal controls. Additionally, it should include an analysis of the applicable privacy laws and regulations. This audit will provide you with an objective third-party assessment of your organization\\'s compliance with international privacy standards and identify any areas of non-compliance that need to be addressed

QUESTION 6

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.”

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.

If the vendor\\'s actions raise concerns about privacy protection, what action should you take first?

A. Review the vendor selection process to see what may have been overlooked.

B. Convene the privacy team to discuss your suspicions.

C. Investigate to ensure that customer data is secure.

D. Phone the vendor to share your concerns.

Correct Answer: D

QUESTION 7

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 8

As a Data Protection Officer, one of your roles entails monitoring changes in laws and regulations and updating policies accordingly.

How would you most effectively execute this responsibility?

A. Consult an external lawyer.

B. Regularly engage regulators.

C. Attend workshops and interact with other professionals.

D. Subscribe to email list-serves that report on regulatory changes.

Correct Answer: D

QUESTION 9

SCENARIO

Please use the following to answer the next QUESTION:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production ?not data processing ?and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company\\'s relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.

To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth ?his uncle\\'s vice president and longtime confidante ?wants to hold off on Anton\\'s idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password- protected system that only he and Kenneth can access.

Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton\\'s possession can be destroyed within the next few years.

After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question are not cause for concern; all of the data was encrypted and not sensitive in

nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.

Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company\\'s online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.

Documentation of this analysis will show auditors due diligence.

Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle\\'s legacy to continue for many years to come.

Which of Anton\\'s plans for improving the data management of the company is most unachievable?

A. His initiative to achieve regulatory compliance.

B. His intention to transition to electronic storage.

C. His objective for zero loss of personal information.

D. His intention to send notice letters to customers and employees.

Correct Answer: A

QUESTION 10

Post-liquidation, a company that has acquired assets would require separate consent from a data subject if personally identifiable data were being retained for which purpose?

A. For tax purposes.

B. For analytical purposes.

C. To be able to ensure payment of pension funds.

D. To secure employment benefits for former employees.

Correct Answer: B

QUESTION 11

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 12

What should a privacy professional keep in mind when selecting which metrics to collect?

A. Metrics should be reported to the public.

B. The number of metrics should be limited at first.

C. Metrics should reveal strategies for increasing company earnings.

D. A variety of metrics should be collected before determining their specific functions.

Correct Answer: A

QUESTION 13

Which of the following best supports implementing controls to bring privacy policies into effect?

A. The internal audit department establishing the audit controls which test for policy effectiveness.

B. The legal department or outside counsel conducting a thorough review of the privacy program and policies.

C. The Chief Information Officer as part of the Senior Management Team creating enterprise privacy policies to ensure controls are available.

D. The information technology (IT) group supporting and enhancing the privacy program and privacy policy by developing processes and controls.

Correct Answer: A

QUESTION 14

SCENARIO

Please use the following to answer the next QUESTION:

Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company\\'s flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to

manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.

The packaging and user guide for the Handy Helper indicate that it is a "privacy friendly" product suitable for the whole

family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family

creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected

marketing partners in order to be able to use the application.

Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Questions about the product from the distributor. Sanjay needed to look more closely

at the product in order to be able to answer the Questions as he was not involved in the product development process.

In speaking with the product team, he learned that the Handy Helper collected and stored all of a user\\'s sensitive medical information for the medical appointment scheduler. In fact, all of the user\\'s information is stored by Handy Helper for the

additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.

Consistent with the CEO\\'s philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some

point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.

What administrative safeguards should be implemented to protect the collected data while in use by Manasa and her product management team?

A. Document the data flows for the collected data.

B. Conduct a Privacy Impact Assessment (PIA) to evaluate the risks involved.

C. Implement a policy restricting data access on a "need to know" basis.

D. Limit data transfers to the US by keeping data collected in Europe within a local data center.

Correct Answer: A

QUESTION 15

Which will best assist you in quickly identifying weaknesses in your network and storage?

A. Running vulnerability scanning tools.

B. Reviewing your privacy program metrics.

C. Reviewing your role-based access controls.

D. Establishing a complaint-monitoring process.

Correct Answer: A