DUMPSARENA

Certified Information Privacy Manager (CIPM)

IAPP CIPM

Version Demo

Total Demo Questions: 10

Total Premium Questions: 166

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

SCENARIO

Please use the following to answer the next QUESTION:

Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather's law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office's strategies for growth.

Immediately upon arrival, Richard was amazed at the amount of work that needed to done in order to modernize the office, mostly in regard to the handling of clients' personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place Richard is also concerned with the overuse of the communal copier/ printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year's end.

Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary Mr. McAdams granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.

As Richard begins to research more about Data Lifecycle Management (DLM), he discovers that the law office can lower the risk of a data breach by doing what?

A. Prioritizing the data by order of importance.

B. Minimizing the time it takes to retrieve the sensitive data.

C. Reducing the volume and the type of data that is stored in its system.

D. Increasing the number of experienced staff to code and categorize the incoming data.

ANSWER: C

QUESTION NO: 2

SCENARIO

Please use the following to answer the next QUESTION:

As they company’s new chief executive officer, Thomas Goddard wants to be known as a leader in data

protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically

Questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that "appropriate" data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.

Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. "We want Medialite to have absolutely the highest standards," he says. "In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective."

You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.

What metric can Goddard use to assess whether costs associated with implementing new privacy protections are justified?

A. Compliance ratio

B. Cost-effective mean

C. Return on investment

D. Implementation measure

ANSWER: C

QUESTION NO: 3

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.

ANSWER: A

QUESTION NO: 4

An organization is establishing a mission statement for its privacy program. Which of the following statements would be the best to use?

A. This privacy program encourages cross-organizational collaboration which will stop all data breaches

B. Our organization was founded in 2054 to reduce the chance of a future disaster like the one that occurred ten years ago. All individuals from our area of the country should be concerned about a future disaster. However, with our privacy program, they should not be concerned about the misuse of their information.

C. The goal of the privacy program is to protect the privacy of all individuals who support our organization. To meet this goal, we must work to comply with all applicable privacy laws.

D. In the next 20 years, our privacy program should be able to eliminate 80% of our current breaches. To do this, everyone in our organization must complete our annual privacy training course and all personally identifiable information must be inventoried.

ANSWER: C

QUESTION NO: 5

What is a key feature of the privacy metric template adapted from the National Institute of Standards and Technology (NIST)?

A. It provides suggestions about how to collect and measure data.

B. It can be tailored to an organization's particular needs.

C. It is updated annually to reflect changes in government policy.

D. It is focused on organizations that do business internationally.

ANSWER: A

QUESTION NO: 6

The General Data Protection Regulation (GDPR) specifies fines that may be levied against data controllers for certain infringements. Which of the following will be subject to administrative fines of up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year?

A. Failure to demonstrate that consent was given by the data subject to the processing of their personal data where it is used as the basis for processing

B. Failure to implement technical and organizational measures to ensure data protection is enshrined by design and default

C. Failure to process personal information in a manner compatible with its original purpose

D. Failure to provide the means for a data subject to rectify inaccuracies in personal data

ANSWER: A

Explanation:

Reference: https://gdpr-info.eu/art-8-gdpr

QUESTION NO: 7

SCENARIO

Please use the following to answer the next QUESTION:

As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically Questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that "appropriate" data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.

Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures.

He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. "We want Medialite to have absolutely the highest standards," he says. "In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective."

You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.

You give a presentation to your CEO about privacy program maturity. What does it mean to have a "managed" privacy program, according to the AICPA/CICA Privacy Maturity Model?

A. Procedures or processes exist, however they are not fully documented and do not cover all relevant aspects.

B. Procedures and processes are fully documented and implemented, and cover all relevant aspects.

C. Reviews are conducted to assess the effectiveness of the controls in place.

D. Regular review and feedback are used to ensure continuous improvement toward optimization of the given process.

ANSWER: C

Explanation:

Reference: https://vvena.nl/wp-content/uploads/2018/04/aicpa_cica_privacy_maturity_model.pdf (page 2, 4th point under privacy maturity model)

QUESTION NO: 8

An organization's internal audit team should do all of the following EXCEPT?

A. Implement processes to correct audit failures.

B. Verify that technical measures are in place.

C. Review how operations work in practice.

D. Ensure policies are being adhered to.

ANSWER: B

QUESTION NO: 9

"Respond" in the privacy operational lifecycle includes which of the following?

A. Information security practices and functional area integration.

B. Privacy awareness training and compliance monitoring.

C. Communication to stakeholders and alignment to laws.

D. Information requests and privacy rights requests.

ANSWER: D

QUESTION NO: 10

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.

Which of the following elements of the incident did you adequately determine?

A. The nature of the data elements impacted

B. The likelihood the incident may lead to harm

C. The likelihood that the information is accessible and usable

D. The number of individuals whose information was affected

ANSWER: B