Free Questions for CIPM

Shared by Albert on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SCENARIO

Please use the following to answer the next QUESTION:

Paul Daniels, with years of experience as a CEO, is worried about his son Carlton's successful venture, Gadgo. A technological innovator in the communication industry that quickly became profitable, Gadgo has moved beyond its startup phase. While it has retained its vibrant energy, Paul fears that under Carlton's

direction, the company may not be taking its risks or obligations as seriously as it needs to. Paul has hired you, a Privacy Consultant, to assess the company and report to both father and son. "Carlton won't listen to me," Paul says, "but he may pay attention to an expert."

Gadgo's workplace is a clubhouse for innovation, with games, toys, snacks. espresso machines, giant fish tanks and even an iguana who regards you with little interest. Carlton, too, seems bored as he describes to you the company's procedures and technologies for data protection. It's a loose assemblage of controls, lacking consistency and with plenty of weaknesses. "This is a technology company," Carlton says. "We create. We innovate. I don't want unnecessary measures that will only slow people down and clutter their thoughts."

The meeting lasts until early evening. Upon leaving, you walk through the office it looks as if a strong windstorm has recently blown through, with papers scattered across desks and tables and even the floor. A "cleaning crew" of one teenager is emptying the trash bins. A few computers have been left on for the night, others are missing. Carlton takes note of your attention to this: "Most of my people take their laptops home with them, or use their own tablets or phones. I want them to use whatever helps them to think and be ready day or night for that great insight. It may only come once!"

What phase in the Privacy Maturity Model (PMM) does Gadgo's privacy program best exhibit?

Options:

A- Ad hoc.
B- Defined.
C- Repeatable.
D- Managed.

Answer:

A

Explanation:

This answer is the best way to describe the phase in the Privacy Maturity Model (PMM) that Gadgo's privacy program best exhibits, as it shows that the company has no formal or consistent approach to privacy protection and that its privacy practices are largely reactive, unplanned and uncoordinated. The ad hoc phase is the lowest level of maturity in the PMM, which is a framework that measures the effectiveness and maturity of an organization's privacy program based on five phases: ad hoc, repeatable, defined, managed and optimized.The ad hoc phase indicates that the organization has little or no awareness of its privacy obligations and risks, and that its privacy activities are dependent on individual efforts or initiatives, rather than on organizational policies or processes.Reference: IAPP CIPM Study Guide, page 891; ISO/IEC 27002:2013, section 18.1.1

Question 2

Question Type: MultipleChoice

When conducting due diligence during an acquisition, what should a privacy professional avoid?

Options:

A- Discussing with the acquired company the type and scope of their data processing.
B- Allowing legal in both companies to handle the privacy laws and compliance.
C- Planning for impacts on the data processing operations post-acquisition.
D- Benchmarking the two Companies privacy policies against one another.

Answer:

B

Explanation:

When conducting due diligence during an acquisition, a privacy professional should avoid allowing legal in both companies to handle the privacy laws and compliance. This is because privacy is not only a legal issue, but also a business, technical, and operational issue that requires cross-functional collaboration and expertise. A privacy professional should be involved in the due diligence process to assess the privacy risks and opportunities of the acquisition, such as the type and scope of data processing, the data protection policies and practices, the data transfer mechanisms and agreements, the data breach history and response plans, and the impacts on the data processing operations post-acquisition. A privacy professional should also benchmark the two companies' privacy policies against one another to identify any gaps or inconsistencies that need to be addressed before or after the acquisition, .Reference:[CIPM -

International Association of Privacy Professionals], [Free CIPM Study Guide - International Association of Privacy Professionals]

Question 3

Question Type: MultipleChoice

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

Options:

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

Explanation:

An organization's mission statement for its privacy program should be concise, clear, and realistic. It should communicate the purpose and scope of the program, as well as the values and principles that guide it. It should also reflect the organization's culture and identity, and align with its strategic objectives. Out of the four options, statement C is the best one to use because it expresses the goal of protecting the privacy of all individuals who support the organization, and acknowledges the need to comply with all applicable privacy laws. The other statements are either too vague, too specific, too ambitious, or too irrelevant for a mission statement.Reference:IAPP CIPM Study Guide, page 18.

Question 4

Question Type: MultipleChoice

Which of the following best demonstrates the effectiveness of a firm's privacy incident response process?

Options:

A- The decrease of security breaches
B- The decrease of notifiable breaches
C- The increase of privacy incidents reported by users
D- The decrease of mean time to resolve privacy incidents

Answer:

D

Explanation:

The decrease of mean time to resolve privacy incidents best demonstrates the effectiveness of a firm's privacy incident response process. This metric measures how quickly and efficiently the firm can identify, contain, analyze, remediate, and report privacy incidents. A lower mean time to resolve indicates a higher level of preparedness, responsiveness, and resilience in handling privacy incidents.Reference:IAPP CIPM Study Guide, page 25.

Question 5

Question Type: MultipleChoice

When supporting the business and data privacy program expanding into a new jurisdiction, it is important to do all of the following EXCEPT?

Options:

A- Identify the stakeholders.
B- Appoint a new Privacy Officer (PO) for that jurisdiction.
C- Perform an assessment of the laws applicable in that new jurisdiction.
D- Consider culture and whether the privacy framework will need to account for changes in

culture.

Answer:

B

Explanation:

When expanding into a new jurisdiction, it is not necessary to appoint a new Privacy Officer (PO) for that jurisdiction, unless the local law requires it. The other options are important steps to ensure compliance with the new jurisdiction's privacy laws and regulations, as well as to align the privacy program with the business objectives and culture of the new market.Reference:CIPM Body of Knowledge, Domain I: Privacy Program Governance, Task 1: Establish the privacy program vision and strategy.

Question 6

Question Type: MultipleChoice

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?

Options:

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:

B

Explanation:

The GDPR specifies fines that may be levied against data controllers for certain infringements.

According to Article 83(4)(a) of the GDPR, failure to implement technical and organizational measures to ensure data protection is enshrined by design and default 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, whichever is higher. Data protection by design and default is a principle that requires data controllers to integrate data protection considerations into every stage of the processing activities, from the conception to the execution, and to adopt appropriate measures to safeguard the rights and interests of the data subjects by default, such as minimizing the amount and retention period of personal data, pseudonymizing or encrypting personal data, ensuring transparency and accountability, and enabling data subject rights.

CIPM Body of Knowledge (2021), Domain I: Privacy Program Governance, Section A: Privacy Governance Models, Subsection 2: Privacy by Design

CIPM Study Guide (2021), Chapter 2: Privacy Governance Models, Section 2.2: Privacy by Design

CIPM Textbook (2019), Chapter 2: Privacy Governance Models, Section 2.2: Privacy by Design

CIPM Practice Exam (2021), Question 130

GDPR Article 83(4)(a) and Article 25

Question 7

Question Type: MultipleChoice

While trying to e-mail her manager, an employee has e-mailed a list of all the company's customers, including their bank details, to an employee with the same name at a different company. Which of the following would be the first stage in the incident response plan under the General Data Protection Regulation (GDPR)?

Options:

A- Notification to data subjects.
B- Containment of impact of breach.
C- Remediation offers to data subjects.
D- Notification to the Information Commissioner's Office (ICO).

Answer:

B

Explanation:

The first stage in the incident response plan under the General Data Protection Regulation (GDPR) for this scenario would be to contain the impact of the breach. This means taking immediate action to stop the unauthorized access or disclosure of personal data, and to prevent it from happening again in the future. This could involve revoking access to the data, notifying the employee who mistakenly sent the data, and implementing security measures to prevent similar breaches from occurring in the future.

https://gdpr-info.eu/art-33-gdpr/

https://gdpr-info.eu/art-34-gdpr/

Question 8

Question Type: MultipleChoice

SCENARIO

Please use the following to answer the next QUESTION:

Martin Briseo is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseo 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 Briseo 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 Briseo'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. Briseo 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.

In the Information Technology engineers had originally set the default for customer credit card information to ''Do Not Save,'' this action would have been in line with what concept?

Options:

A- Use limitation
B- Privacy by Design
C- Harm minimization
D- Reactive risk management

Answer:

B

Question 9

Question Type: MultipleChoice

A minimum requirement for carrying out a Data Protection Impact Assessment (DPIA) would include?

Options:

A- Processing on a large scale of special categories of data.
B- Monitoring of a publicly accessible area on a large scale.
C- Assessment of the necessity and proportionality.
D- Assessment of security measures.

Answer:

A

Explanation:

Processing on a large scale of special categories of data is a minimum requirement for carrying out a Data Protection Impact Assessment (DPIA) under the General Data Protection Regulation (GDPR). A DPIA is a type of Privacy Impact Assessment (PIA) that is specifically required by the GDPR when a processing activity is likely to result in a high risk to the rights and freedoms of natural persons. According to Article 35(3)(b) of the GDPR, a DPIA is mandatory when the processing involves a large scale of special categories of data or personal data relating to criminal convictions and offences. Special categories of data are personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation. These types of data are considered more sensitive and require more protection, as they may pose higher risks of discrimination, identity theft, fraud, or other harms to the data subjects.

CIPM Body of Knowledge (2021), Domain IV: Privacy Program Operational Life Cycle, Section C: Monitoring and Managing Program Performance Subsection 1: Privacy Impact Assessments

CIPM Study Guide (2021), Chapter 9: Monitoring and Managing Program Performance Section 9.1: Privacy Impact Assessments

CIPM Textbook (2019), Chapter 9: Monitoring and Managing Program Performance Section 9.1: Privacy Impact Assessments

CIPM Practice Exam (2021), Question 147

GDPR Article 35(3)(b) and Article 9

Question 10

Question Type: MultipleChoice

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 was done CORRECTLY during the above incident?

Options:

A- The process by which affected individuals sign up for email notifications
B- Your assessment of which credit monitoring company you should hire
C- The speed at which you sat down to reflect and document the incident
D- Finding a vendor who will offer the affected individuals additional services

Answer:

C

Explanation:

This answer is the only thing that was done correctly during the incident, as it shows a good practice of learning from and improving on the incident response process. The speed at which you sat down to reflect and document the incident means that you did not delay or postpone this important step, which can help you to capture and analyze what went well and what could have gone better during the incident, as well as to identify any lessons learned, best practices or recommendations for future incidents. Documenting and reflecting on the incident can also help you to update and improve your privacy policies, procedures and safeguards, as well as to demonstrate your accountability and compliance with any legal or contractual obligations.