Free Questions for CIPM

Shared by Spears on 04-10-2024

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:

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.

How was Pacific Suites responsible for protecting the sensitive information of its offshoot, PHT?

Options:

A- As the parent company, it should have transferred personnel to oversee the secure handling of PHT's data.
B- As the parent company, it should have performed an assessment of PHT's infrastructure and confirmed complete separation of the two networks.
C- As the parent company, it should have ensured its existing data access and storage procedures were integrated into PHT's system.
D- As the parent company, it should have replaced PHT's electronic files with hard-copy documents stored securely on site.

Answer:

C

Question 2

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 would be the best kind of audit to recommend for Gadgo?

Options:

A- A supplier audit.
B- An internal audit.
C- A third-party audit.
D- A self-certification.

Answer:

C

Explanation:

This answer is the best kind of audit to recommend for Gadgo, as it can provide an independent and objective assessment of the company's privacy program and practices, as well as identify any gaps, weaknesses or risks that need to be addressed or improved. A third-party audit is conducted by an external auditor who has the necessary expertise, experience and credentials to evaluate the company's compliance with the applicable laws, regulations, standards and best practices for data protection.A third-party audit can also help to enhance the company's reputation and trust among its customers, partners and stakeholders, as well as demonstrate its commitment and accountability for privacy protection.Reference: IAPP CIPM Study Guide, page 881; ISO/IEC 27002:2013, section 18.2.1

Question 3

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.

What must Pacific Suite's primary focus be as it manages this security breach?

Options:

A- Minimizing the amount of harm to the affected individuals
B- Investigating the cause and assigning responsibility
C- Determining whether the affected individuals should be notified
D- Maintaining operations and preventing publicity

Answer:

A

Question 4

Question Type: MultipleChoice

Your marketing team wants to know why they need a check box for their SMS opt-in. You explain it is part of the consumer's right to?

Options:

A- Request correction.
B- Raise complaints.

C- Have access.
D- Be informed.

Answer:

D

Explanation:

The marketing team needs a check box for their SMS opt-in because it is part of the consumer's right to be informed. This right means that consumers have the right to know how their personal data is collected, used, shared, and protected by the organization. The check box allows consumers to give their consent and opt-in to receive SMS messages from the organization, and also informs them of the purpose and scope of such messages. The other rights are not relevant in this case, as they are related to other aspects of data processing, such as correction, complaints, and access.Reference:CIPM Body of Knowledge, Domain IV: Privacy Program Communication, Section A: Communicating to Stakeholders, Subsection 1: Consumer Rights.

Question 5

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 elements of the incident did you adequately determine?

Options:

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:

D

Explanation:

This answer is the only element of the incident that you adequately determined, as you knew exactly how many people were impacted by the vendor's data loss and you communicated this number to them in the notification. The other elements of the incident were not adequately determined, as you did not:

Assess the nature of the data elements impacted, such as what type, category, sensitivity or value of data was involved, and how it could affect the individuals' privacy, security or identity.

Evaluate the likelihood that the incident may lead to harm, such as financial, reputational, emotional or physical harm to the individuals or the organization, and how severe or widespread the harm could be.

Estimate the likelihood that the information is accessible and usable, such as who may have access to or control over the data, and how they may use or misuse it for malicious or fraudulent purposes.

Question 6

Question Type: MultipleChoice

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.

What is the best way for your vendor to be clear about the Society's breach notification expectations?

Options:

A- Include notification provisions in the vendor contract
B- Arrange regular telephone check-ins reviewing expectations
C- Send a memorandum of understanding on breach notification
D- Email the regulations that require breach notifications

Answer:

A

Explanation:

This answer is the best way for Albert's vendor to be clear about the Society's breach notification expectations, as it can establish clear and binding terms and conditions for both parties regarding their roles and responsibilities for handling any data security incidents or breaches. Including notification provisions in the vendor contract can help to define what constitutes a breach, how it should be detected, reported and investigated, what information should be provided to the organization and within what time frame, what actions should be taken to mitigate or resolve the breach, and what consequences or liabilities may arise from the breach. The contract can also specify that the vendor must cooperate and coordinate with the organization in any breach notification activities to the relevant authorities, customers, partners

or stakeholders.

Question 7

Question Type: MultipleChoice

Under which circumstances would people who work in human resources be considered a secondary audience for privacy metrics?

Options:

A- They do not receive training on privacy issues
B- They do not interface with the financial office
C- They do not have privacy policy as their main task
D- They do not have frequent interactions with the public

Answer:

C

Explanation:

People who work in human resources would be considered a secondary audience for privacy metrics if they do not have privacy policy as their main task. A secondary audience is a group of stakeholders who are indirectly involved or affected by the privacy program, but do not have primary responsibility or authority over it. They may use privacy metrics to support their own functions or objectives, such as hiring, training, or compliance.Reference:IAPP CIPM Study Guide, page 23.

Question 8

Question Type: MultipleChoice

Which term describes a piece of personal data that alone may not identify an individual?

Options:

A- Unbundled data
B- A singularity
C- Non-aggregated infopoint
D- A single attribute

Answer:

D

Explanation:

A single attribute is a term that describes a piece of personal data that alone may not identify an individual, such as a first name or a zip code. However, when combined with other attributes, it may become identifiable.Reference:IAPP CIPM Study Guide, page 18.

Question 9

Question Type: MultipleChoice

Which is the best way to view an organization's privacy framework?

Options:

A- As an industry benchmark that can apply to many organizations
B- As a fixed structure that directs changes in the organization
C- As an aspirational goal that improves the organization
D- As a living structure that aligns to changes in the organization

Answer:

D

Explanation:

The best way to view an organization's privacy framework is as a living structure that aligns to changes in the organization, such as business goals, stakeholder expectations, legal requirements, and technological developments. A privacy framework should be flexible and adaptable to support the organization's privacy strategy and vision. It should also be compatible with other frameworks, such as the cybersecurity framework, that the organization may use.Reference:IAPP CIPM Study Guide, page 16.

Question 10

Question Type: MultipleChoice

An executive for a multinational online retail company in the United States is looking for guidance in developing her company's privacy program beyond what is specifically required by law.

What would be the most effective resource for the executive to consult?

Options:

A- Internal auditors.
B- Industry frameworks.
C- Oversight organizations.
D- Breach notifications from competitors.

Answer:

B

Explanation:

Industry frameworks are the most effective resource for an executive who wants to develop her company's privacy program beyond what is specifically required by law. Industry frameworks are collections of best practices, standards, and guidelines that help organizations establish and improve their privacy policies and procedures. Industry frameworks can help organizations demonstrate their commitment to privacy, enhance their reputation and trustworthiness, and comply with multiple privacy regulations.Some examples of industry frameworks are the NIST Privacy Framework2, the ISO 27701 Privacy Information Management System3, and the AICPA/CICA Generally Accepted Privacy Principles (GAPP)4. The other options are not as effective as industry frameworks for developing a privacy program. Internal auditors can help evaluate the effectiveness and compliance of existing privacy controls, but they may not provide guidance on how to improve or expand them. Oversight organizations can enforce privacy laws and regulations, but they may not offer advice on how to go beyond the legal requirements. Breach notifications from competitors can alert organizations to potential threats and vulnerabilities, but they may not suggest how to prevent or mitigate them.Reference:NIST Privacy Framework;ISO 27701 Privacy Information Management System;AICPA/CICA Generally Accepted Privacy Principles (GAPP)