

## Exam Questions CIPM

Certified Information Privacy Manager (CIPM)

<https://www.2passeasy.com/dumps/CIPM/>



### NEW QUESTION 1

#### SCENARIO

Please use the following to answer the next QUESTION:

For 15 years, Albert has worked at Treasure Box – a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountants)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public is unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers.

For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

In consideration of the company's new initiatives, which of the following laws and regulations would be most appropriate for Albert to mention at the interview as a priority concern for the privacy team?

- A. Gramm-Leach-Bliley Act (GLBA)
- B. The General Data Protection Regulation (GDPR)
- C. The Telephone Consumer Protection Act (TCPA)
- D. Health Insurance Portability and Accountability Act (HIPAA)

**Answer: B**

### NEW QUESTION 2

#### SCENARIO

Please use the following to answer the next QUESTION:

John is the new privacy officer at the prestigious international law firm – A&M LLP. A&M LLP is very proud of its reputation in the practice areas of Trusts & Estates and Merger & Acquisition in both U.S. and Europe.

During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm's email continuity service to their existing email security vendor – MessageSafe. Being successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from Cloud Inc. to host email continuity service for A&M LLP.

John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe's previous breach and learned that the breach was caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.

At the meeting, Derrick emphasized that email is the primary method for the firm's lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn't have the time or resource to look for another solution. Furthermore, the off-premises email continuity service will only be turned on when the email service at A&M LLP's primary and secondary data centers are both down, and the email messages stored at MessageSafe site for continuity service will be automatically deleted after 30 days.

Which of the following is a TRUE statement about the relationship among the organizations?

- A. Cloud Inc.
- B. must notify A&M LLP of a data breach immediately.
- C. MessageSafe is liable if Cloud Inc.
- D. fails to protect data from A&M LLP.
- E. Cloud Inc.
- F. should enter into a data processor agreement with A&M LLP.
- G. A&M LLP's service contract must be amended to list Cloud Inc.
- H. as a sub-processor.

**Answer: A**

### NEW QUESTION 3

In privacy protection, what is a "covered entity"?

- A. Personal data collected by a privacy organization.
- B. An organization subject to the privacy provisions of HIPAA.
- C. A privacy office or team fully responsible for protecting personal information.
- D. Hidden gaps in privacy protection that may go unnoticed without expert analysis.

**Answer: B**

### NEW QUESTION 4

**SCENARIO**

Please use the following to answer the next QUESTION:

Martin Briseño is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseño 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 Briseño 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 Briseño'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. Briseño 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 key mistake set the company up to be vulnerable to a security breach?

- A. Collecting too much information and keeping it for too long
- B. Overlooking the need to organize and categorize data
- C. Failing to outsource training and data management to professionals
- D. Neglecting to make a backup copy of archived electronic files

**Answer: B**

**NEW QUESTION 5****SCENARIO**

Please use the following to answer the next QUESTION:

Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.

With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.

Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.

Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.

Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.

Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.

What Data Lifecycle Management (DLM) principle should the company follow if they end up allowing departments to interpret the privacy policy differently?

- A. Prove the authenticity of the company's records.
- B. Arrange for official credentials for staff members.
- C. Adequately document reasons for inconsistencies.
- D. Create categories to reflect degrees of data importance.

**Answer: C**

**NEW QUESTION 6**

Which of the following privacy frameworks are legally binding?

- A. Binding Corporate Rules (BCRs).
- B. Generally Accepted Privacy Principles (GAPP).
- C. Asia-Pacific Economic Cooperation (APEC) Privacy Framework.
- D. Organization for Economic Co-Operation and Development (OECD) Guidelines.

**Answer: A**



## NEW QUESTION 7

### 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?

- 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

## NEW QUESTION 8

An organization's privacy officer was just notified by the benefits manager that she accidentally sent out the retirement enrollment report of all employees to a wrong vendor.

Which of the following actions should the privacy officer take first?

- A. Perform a risk of harm analysis.
- B. Report the incident to law enforcement.
- C. Contact the recipient to delete the email.
- D. Send firm-wide email notification to employees.

**Answer:** A

## NEW QUESTION 9

### 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.

Regarding the notification, which of the following would be the greatest concern?

- A. Informing the affected individuals that data from other individuals may have also been affected.
- B. Collecting more personally identifiable information than necessary to provide updates to the affected individuals.
- C. Using a postcard with the logo of the vendor who make the mistake instead of your company's logo.
- D. Trusting a vendor to send out a notice when they already failed once by not encrypting the database.

**Answer:** D

#### NEW QUESTION 10

What is the name for the privacy strategy model that describes delegated decision making?

- A. De-centralized.
- B. De-functionalized.
- C. Hybrid.
- D. Matrix.

**Answer:** A

#### NEW QUESTION 10

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

- 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:** B

#### NEW QUESTION 11

In a sample metric template, what does "target" mean?

- A. The suggested volume of data to collect
- B. The percentage of completion
- C. The threshold for a satisfactory rating
- D. The frequency at which the data is sampled

**Answer:** A

#### NEW QUESTION 13

Which of the following controls does the PCI DSS framework NOT require?

- A. Implement strong asset control protocols.
- B. Implement strong access control measures.
- C. Maintain an information security policy.
- D. Maintain a vulnerability management program.

**Answer:** A

#### NEW QUESTION 16

##### SCENARIO

Please use the following to answer the next QUESTION:

For 15 years, Albert has worked at Treasure Box – a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountants)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public is unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers.

For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

On which of the following topics does Albert most likely need additional knowledge?

- A. The role of privacy in retail companies
- B. The necessary maturity level of privacy programs
- C. The possibility of delegating responsibilities related to privacy
- D. The requirements for a managerial position with privacy protection duties

**Answer:** C

### NEW QUESTION 17

#### SCENARIO

Please use the following to answer the next QUESTION:

For 15 years, Albert has worked at Treasure Box – a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountants)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public is unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers.

For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

Based on Albert's observations regarding recent security incidents, which of the following should he suggest as a priority for Treasure Box?

- A. Appointing an internal ombudsman to address employee complaints regarding hours and pay.
- B. Using a third-party auditor to address privacy protection issues not recognized by the prior internal audits.
- C. Working with the Human Resources department to make screening procedures for potential employees more rigorous.
- D. Evaluating the company's ability to handle personal health information if the plan to acquire the medical supply company goes forward

**Answer: D**

### NEW QUESTION 22

What is the main purpose of a privacy program audit?

- A. To mitigate the effects of a privacy breach.
- B. To justify a privacy department budget increase.
- C. To make decisions on privacy staff roles and responsibilities.
- D. To ensure the adequacy of data protection procedures.

**Answer: D**

### NEW QUESTION 23

#### SCENARIO

Please use the following to answer the next QUESTION:

As the 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.

The company has achieved a level of privacy protection that established new best practices for the industry. What is a logical next step to help ensure a high level of protection?

- A. Brainstorm methods for developing an enhanced privacy framework
- B. Develop a strong marketing strategy to communicate the company's privacy practices
- C. Focus on improving the incident response plan in preparation for any breaks in protection
- D. Shift attention to privacy for emerging technologies as the company begins to use them

**Answer: C**

### NEW QUESTION 27

When implementing Privacy by Design (PbD), what would NOT be a key consideration?

- A. Collection limitation.
- B. Data minimization.
- C. Limitations on liability.



D. Purpose specification.

**Answer:** C

### NEW QUESTION 32

#### 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.

Regarding the credit monitoring, which of the following would be the greatest concern?

- A. The vendor's representative does not have enough experience
- B. Signing a contract with CRUDLOK which lasts longer than one year
- C. The company did not collect enough identifiers to monitor one's credit
- D. You are going to notify affected individuals via a letter followed by an email

**Answer:** A

### NEW QUESTION 37

#### SCENARIO

Please use the following to answer the next QUESTION:

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

- 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

#### NEW QUESTION 42

##### SCENARIO

Please use the following to answer the next QUESTION:

Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.

This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them."

Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!"

What safeguard can most efficiently ensure that privacy protection is a dimension of relationships with vendors?

- A. Include appropriate language about privacy protection in vendor contracts.
- B. Perform a privacy audit on any vendor under consideration.
- C. Require that a person trained in privacy protection be part of all vendor selection teams.
- D. Do business only with vendors who are members of privacy trade associations.

**Answer:** C

#### NEW QUESTION 45

In which situation would a Privacy Impact Assessment (PIA) be the least likely to be required?

- A. If a company created a credit-scoring platform five years ago.
- B. If a health-care professional or lawyer processed personal data from a patient's file.
- C. If a social media company created a new product compiling personal data to generate user profiles.
- D. If an after-school club processed children's data to determine which children might have food allergies.

**Answer:** D

#### NEW QUESTION 50

Under the General Data Protection Regulation (GDPR), when would a data subject have the right to require the erasure of his or her data without undue delay?

- A. When the data subject is a public authority.
- B. When the erasure is in the public interest.
- C. When the processing is carried out by automated means.
- D. When the data is no longer necessary for its original purpose.

**Answer:** A

#### NEW QUESTION 52

##### SCENARIO

Please use the following to answer the next QUESTION:

Penny has recently joined Ace Space, a company that sells homeware accessories online, as its new privacy officer. The company is based in California but thanks to some great publicity from a social media influencer last year, the company has received an influx of sales from the EU and has set up a regional office in Ireland to support this expansion. To become familiar with Ace Space's practices and assess what her privacy priorities will be, Penny has set up meetings with a number of colleagues to hear about the work that they have been doing and their compliance efforts.

Penny's colleague in Marketing is excited by the new sales and the company's plans, but is also concerned that Penny may curtail some of the growth opportunities he has planned. He tells her "I heard someone in the breakroom talking about some new privacy laws but I really don't think it affects us. We're just a small company. I mean we just sell accessories online, so what's the real risk?" He has also told her that he works with a number of small companies that help him get projects completed in a hurry. "We've got to meet our deadlines otherwise we lose money. I just sign the contracts and get Jim in finance to push through the payment. Reviewing the contracts takes time that we just don't have."

In her meeting with a member of the IT team, Penny has learned that although Ace Space has taken a number of precautions to protect its website from malicious activity, it has not taken the same level of care of its physical files or internal infrastructure. Penny's colleague in IT has told her that a former employee lost an encrypted USB key with financial data on it when he left. The company nearly lost access to their customer database last year after they fell victim to a phishing attack. Penny is told by her IT colleague that the IT team "didn't know what to do or who should do what. We hadn't been trained on it but we're a small team though, so it worked out OK in the end." Penny is concerned that these issues will compromise Ace Space's privacy and data protection.

Penny is aware that the company has solid plans to grow its international sales and will be working closely with the CEO to give the organization a data "shake up". Her mission is to cultivate a strong privacy culture within the company.

Penny has a meeting with Ace Space's CEO today and has been asked to give her first impressions and an overview of her next steps.

What is the best way for Penny to understand the location, classification and processing purpose of the personal data Ace Space has?

- A. Analyze the data inventory to map data flows
- B. Audit all vendors' privacy practices and safeguards



- C. Conduct a Privacy Impact Assessment for the company
- D. Review all cloud contracts to identify the location of data servers used

**Answer:** B

#### NEW QUESTION 56

How are individual program needs and specific organizational goals identified in privacy framework development?

- A. By employing metrics to align privacy protection with objectives.
- B. Through conversations with the privacy team.
- C. By employing an industry-standard needs analysis.
- D. Through creation of the business case.

**Answer:** A

#### NEW QUESTION 60

##### SCENARIO

Please use the following to answer the next QUESTION:

For 15 years, Albert has worked at Treasure Box – a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountants)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public is unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers.

For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

Based on Albert's observations, executive leadership should most likely pay closer attention to what?

- A. Awareness campaigns with confusing information
- B. Obsolete data processing systems
- C. Outdated security frameworks
- D. Potential in-house threats

**Answer:** C

#### NEW QUESTION 64

Which of the following is TRUE about a PIA (Privacy Impact Analysis)?

- A. Any project that involves the use of personal data requires a PIA
- B. A Data Protection Impact Analysis (DPIA) process includes a PIA
- C. The PIA must be conducted at the early stages of the project lifecycle
- D. The results from a previous information audit can be leveraged in a PIA process

**Answer:** A

#### NEW QUESTION 65

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

#### NEW QUESTION 69

Which of the following is an example of Privacy by Design (PbD)?

- A. A company hires a professional to structure a privacy program that anticipates the increasing demands of new laws.
- B. The human resources group develops a training program for employees to become certified in privacy policy.
- C. A labor union insists that the details of employers' data protection methods be documented in a new contract.
- D. The information technology group uses privacy considerations to inform the development of new networking software.

Answer: C

### NEW QUESTION 73

Rationalizing requirements in order to comply with the various privacy requirements required by applicable law and regulation does NOT include which of the following?

- A. Harmonizing shared obligations and privacy rights across varying legislation and/or regulators.
- B. Implementing a solution that significantly addresses shared obligations and privacy rights.
- C. Applying the strictest standard for obligations and privacy rights that doesn't violate privacy laws elsewhere.
- D. Addressing requirements that fall outside the common obligations and rights (outliers) on a case-by-case basis.

Answer: C

### NEW QUESTION 77

#### SCENARIO

Please use the following to answer the next QUESTION:

Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.

This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them."

Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!"

You want to point out that normal protocols have NOT been followed in this matter. Which process in particular has been neglected?

- A. Forensic inquiry.
- B. Data mapping.
- C. Privacy breach prevention.
- D. Vendor due diligence vetting.

Answer: D

### NEW QUESTION 79

What United States federal law requires financial institutions to declare their personal data collection practices?

- A. The Kennedy-Hatch Disclosure Act of 1997.
- B. The Gramm-Leach-Bliley Act of 1999.
- C. SUPCLA, or the federal Superprivacy Act of 2001.
- D. The Financial Portability and Accountability Act of 2006.

Answer: B

### NEW QUESTION 84

#### 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.

Answer: A

#### NEW QUESTION 87

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.

**Answer:** A

#### NEW QUESTION 92

##### 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

#### NEW QUESTION 95

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

- 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

#### NEW QUESTION 97

##### 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.

**Answer:** C



#### NEW QUESTION 100

##### SCENARIO

Please use the following to answer the next QUESTION:

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

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

**Answer: B**

#### NEW QUESTION 103

##### 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?

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

**Answer: A**

#### NEW QUESTION 104

##### SCENARIO

Please use the following to answer the next QUESTION:

It's just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It's a great deal, and after a month, more than half the organization's employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them, potentially carrying personal data to their homes or other unknown locations. It's enough to give you data-protection nightmares, and you've pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.

Today you have in your office a representative of the organization's marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop "safely" tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop

was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.

You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.

Which is the best way to ensure that data on personal equipment is protected?

- A. User risk training.
- B. Biometric security.
- C. Encryption of the data.
- D. Frequent data backups.

**Answer:** A

#### NEW QUESTION 106

##### 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?

Which of the following would be most effectively used as a guide to a systems approach to implementing data protection?

- A. Data Lifecycle Management Standards.
- B. United Nations Privacy Agency Standards.
- C. International Organization for Standardization 9000 Series.
- D. International Organization for Standardization 27000 Series.

**Answer:** D

#### NEW QUESTION 108

Formosa International operates in 20 different countries including the United States and France. What organizational approach would make complying with a number of different regulations easier?

- A. Data mapping.
- B. Fair Information Practices.
- C. Rationalizing requirements.
- D. Decentralized privacy management.

**Answer:** B

#### NEW QUESTION 109

##### SCENARIO

Please use the following to answer the next QUESTION:

It's just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It's a great deal, and after a month, more than half the organization's employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them, potentially carrying personal data to their homes or other unknown locations. It's enough to give you data- protection nightmares, and you've pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.

Today you have in your office a representative of the organization's marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop "safely" tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.

You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.

From a business standpoint, what is the most productive way to view employee use of personal equipment for work-related tasks?

- A. The use of personal equipment is a cost-effective measure that leads to no greater security risks than are always present in a modern organization.
- B. Any computer or other equipment is company property whenever it is used for company business.
- C. While the company may not own the equipment, it is required to protect the business-related data on any equipment used by its employees.
- D. The use of personal equipment must be reduced as it leads to inevitable security risks.

**Answer:** C

#### NEW QUESTION 114

##### SCENARIO

Please use the following to answer the next QUESTION:

John is the new privacy officer at the prestigious international law firm – A&M LLP. A&M LLP is very proud of its reputation in the practice areas of Trusts & Estates and Merger & Acquisition in both U.S. and Europe.

During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm's email continuity service to their existing email security vendor – MessageSafe. Being successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from Cloud Inc. to host email continuity service for A&M LLP.

John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe's previous breach and learned that the breach was caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.

At the meeting, Derrick emphasized that email is the primary method for the firm's lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn't have the time or resource to look for another solution. Furthermore, the off-premises email continuity service will only be turned on when the email service at A&M LLP's primary and secondary data centers are both down, and the email messages stored at MessageSafe site for continuity service will be automatically deleted after 30 days.

Which of the following is the most effective control to enforce MessageSafe's implementation of appropriate technical countermeasures to protect the personal data received from A&M LLP?

- A. MessageSafe must apply due diligence before trusting Cloud Inc.
- B. with the personal data received from A&M LLP.
- C. MessageSafe must flow-down its data protection contract terms with A&M LLP to Cloud Inc.
- D. MessageSafe must apply appropriate security controls on the cloud infrastructure.
- E. MessageSafe must notify A&M LLP of a data breach.

**Answer: D**

#### NEW QUESTION 115

Which statement is FALSE regarding the use of technical security controls?

- A. Technical security controls are part of a data governance strategy.
- B. Technical security controls deployed for one jurisdiction often satisfy another jurisdiction.
- C. Most privacy legislation lists the types of technical security controls that must be implemented.
- D. A person with security knowledge should be involved with the deployment of technical security controls.

**Answer: B**

#### NEW QUESTION 119

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?

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

**Answer: B**

#### NEW QUESTION 120

##### 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 be 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.

Richard needs to closely monitor the vendor in charge of creating the firm's database mainly because of what?

- A. The vendor will be required to report any privacy violations to the appropriate authorities.
- B. The vendor may not be aware of the privacy implications involved in the project.
- C. The vendor may not be forthcoming about the vulnerabilities of the database.
- D. The vendor will be in direct contact with all of the law firm's personal data.

**Answer: B**

#### NEW QUESTION 125



#### SCENARIO

Please use the following to answer the next QUESTION:

Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain "rogue" offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.

In the wake of this incident, Kelly had been sent to Providence to change the "hands off" culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers.

Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.

Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company's license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.

You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.

What should you advise this company regarding the status of security cameras at their offices in the United States?

- A. Add security cameras at facilities that are now without them.
- B. Set policies about the purpose and use of the security cameras.
- C. Reduce the number of security cameras located inside the building.
- D. Restrict access to surveillance video taken by the security cameras and destroy the recordings after a designated period of time.

**Answer: B**

#### NEW QUESTION 130

##### 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 analytic can be used to track the financial viability of the program as it develops?

- A. Cost basis.
- B. Gap analysis.
- C. Return to investment.
- D. Breach impact modeling.

**Answer: C**

#### NEW QUESTION 134

##### 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.

After conducting research, you discover a primary data protection issue with cloud computing. Which of the following should be your biggest concern?

- A. An open programming model that results in easy access
- B. An unwillingness of cloud providers to provide security information

- C. A lack of vendors in the cloud computing market
- D. A reduced resilience of data structures that may lead to data loss.

**Answer:** B

#### NEW QUESTION 139

An organization's business continuity plan or disaster recovery plan does NOT typically include what?

- A. Recovery time objectives.
- B. Emergency response guidelines.
- C. Statement of organizational responsibilities.
- D. Retention schedule for storage and destruction of information.

**Answer:** D

#### NEW QUESTION 143

##### SCENARIO

Please use the following to answer the next QUESTION:

Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.

With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.

Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.

Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.

Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.

Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.

If Amira and Sadie's ideas about adherence to the company's privacy policy go unchecked, the Federal Communications Commission (FCC) could potentially take action against NatGen for what?

- A. Deceptive practices.
- B. Failing to institute the hotline.
- C. Failure to notify of processing.
- D. Negligence in consistent training.

**Answer:** A

#### NEW QUESTION 145

"Collection", "access" and "destruction" are aspects of what privacy management process?

- A. The data governance strategy
- B. The breach response plan
- C. The metric life cycle
- D. The business case

**Answer:** A

#### NEW QUESTION 146

For an organization that has just experienced a data breach, what might be the least relevant metric for a company's privacy and governance team?

- A. The number of security patches applied to company devices.
- B. The number of privacy rights requests that have been exercised.
- C. The number of Privacy Impact Assessments that have been completed.
- D. The number of employees who have completed data awareness training.

**Answer:** A

#### NEW QUESTION 149

##### SCENARIO

Please use the following to answer the next QUESTION:

Penny has recently joined Ace Space, a company that sells homeware accessories online, as its new privacy officer. The company is based in California but thanks to some great publicity from a social media influencer last year, the company has received an influx of sales from the EU and has set up a regional office in Ireland to support this expansion. To become familiar with Ace Space's practices and assess what her privacy priorities will be, Penny has set up meetings with a number of colleagues to hear about the work that they have been doing and their compliance efforts.

Penny's colleague in Marketing is excited by the new sales and the company's plans, but is also concerned that Penny may curtail some of the growth opportunities he has planned. He tells her "I heard someone in the breakroom talking about some new privacy laws but I really don't think it affects us. We're just a small company. I mean we just sell accessories online, so what's the real risk?" He has also told her that he works with a number of small companies that help him get projects completed in a hurry. "We've got to meet our deadlines otherwise we lose money. I just sign the contracts and get Jim in finance to push through

the payment. Reviewing the contracts takes time that we just don't have."

In her meeting with a member of the IT team, Penny has learned that although Ace Space has taken a number of precautions to protect its website from malicious activity, it has not taken the same level of care of its physical files or internal infrastructure. Penny's colleague in IT has told her that a former employee lost an encrypted USB key with financial data on it when he left. The company nearly lost access to their customer database last year after they fell victim to a phishing attack. Penny is told by her IT colleague that the IT team "didn't know what to do or who should do what. We hadn't been trained on it but we're a small team though, so it worked out OK in the end." Penny is concerned that these issues will compromise Ace Space's privacy and data protection.

Penny is aware that the company has solid plans to grow its international sales and will be working closely with the CEO to give the organization a data "shake up". Her mission is to cultivate a strong privacy culture within the company.

Penny has a meeting with Ace Space's CEO today and has been asked to give her first impressions and an overview of her next steps.

To establish the current baseline of Ace Space's privacy maturity, Penny should consider all of the following factors EXCEPT?

- A. Ace Space's documented procedures
- B. Ace Space's employee training program
- C. Ace Space's vendor engagement protocols
- D. Ace Space's content sharing practices on social media

**Answer: A**

#### NEW QUESTION 154

A Human Resources director at a company reported that a laptop containing employee payroll data was lost on the train. Which action should the company take IMMEDIATELY?

- A. Report the theft to law enforcement
- B. Wipe the hard drive remotely
- C. Report the theft to the senior management
- D. Perform a multi-factor risk analysis

**Answer: D**

#### NEW QUESTION 159

##### SCENARIO

Please use the following to answer the next QUESTION:

Penny has recently joined Ace Space, a company that sells homeware accessories online, as its new privacy officer. The company is based in California but thanks to some great publicity from a social media influencer last year, the company has received an influx of sales from the EU and has set up a regional office in Ireland to support this expansion. To become familiar with Ace Space's practices and assess what her privacy priorities will be, Penny has set up meetings with a number of colleagues to hear about the work that they have been doing and their compliance efforts.

Penny's colleague in Marketing is excited by the new sales and the company's plans, but is also concerned that Penny may curtail some of the growth opportunities he has planned. He tells her "I heard someone in the breakroom talking about some new privacy laws but I really don't think it affects us. We're just a small company. I mean we just sell accessories online, so what's the real risk?" He has also told her that he works with a number of small companies that help him get projects completed in a hurry. "We've got to meet our deadlines otherwise we lose money. I just sign the contracts and get Jim in finance to push through the payment. Reviewing the contracts takes time that we just don't have."

In her meeting with a member of the IT team, Penny has learned that although Ace Space has taken a number of precautions to protect its website from malicious activity, it has not taken the same level of care of its physical files or internal infrastructure. Penny's colleague in IT has told her that a former employee lost an encrypted USB key with financial data on it when he left. The company nearly lost access to their customer database last year after they fell victim to a phishing attack. Penny is told by her IT colleague that the IT team "didn't know what to do or who should do what. We hadn't been trained on it but we're a small team though, so it worked out OK in the end." Penny is concerned that these issues will compromise Ace Space's privacy and data protection.

Penny is aware that the company has solid plans to grow its international sales and will be working closely with the CEO to give the organization a data "shake up". Her mission is to cultivate a strong privacy culture within the company.

Penny has a meeting with Ace Space's CEO today and has been asked to give her first impressions and an overview of her next steps.

What information will be LEAST crucial from a privacy perspective in Penny's review of vendor contracts?

- A. Audit rights
- B. Liability for a data breach
- C. Pricing for data security protections
- D. The data a vendor will have access to

**Answer: C**

#### NEW QUESTION 163

What is the main reason to begin with 3-5 key metrics during the program development process?

- A. To avoid undue financial costs.
- B. To keep the focus on the main organizational objectives.
- C. To minimize selective data use.
- D. To keep the process limited to as few people as possible.

**Answer: C**

#### NEW QUESTION 165

##### 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 security controls are missing from the Eureka program?

- A. Storage of medical data in the cloud is not permissible under the General Data Protection Regulation (GDPR)
- B. Data access is not limited to those who "need to know" for their role
- C. Collection of data without a defined purpose might violate the fairness principle
- D. Encryption of the data at rest prevents European users from having the right of access and the right of portability of their data

**Answer: B**

#### NEW QUESTION 166

Which of the following is TRUE about the Data Protection Impact Assessment (DPIA) process as required under the General Data Protection Regulation (GDPR)?

- A. The DPIA result must be reported to the corresponding supervisory authority.
- B. The DPIA report must be published to demonstrate the transparency of the data processing.
- C. The DPIA must include a description of the proposed processing operation and its purpose.
- D. The DPIA is required if the processing activity entails risk to the rights and freedoms of an EU individual.

**Answer: D**

#### NEW QUESTION 171

##### 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 stage of the privacy operational life cycle best describes Consolidated's current privacy program?

- A. Assess.
- B. Protect.
- C. Respond.
- D. Sustain.

**Answer: D**

#### NEW QUESTION 173

##### 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 be 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.

Richard believes that a transition from the use of fax machine to Internet faxing provides all of the following security benefits EXCEPT?

- A. Greater accessibility to the faxes at an off-site location.
- B. The ability to encrypt the transmitted faxes through a secure server.
- C. Reduction of the risk of data being seen or copied by unauthorized personnel.
- D. The ability to store faxes electronically, either on the user's PC or a password-protected network server.

Answer: A

#### NEW QUESTION 174

##### SCENARIO

Please use the following to answer the next QUESTION:

Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain "rogue" offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.

In the wake of this incident, Kelly had been sent to Providence to change the "hands off" culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers.

Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.

Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company's license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.

You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.

What does this example best illustrate about training requirements for privacy protection?

- A. Training needs must be weighed against financial costs.
- B. Training on local laws must be implemented for all personnel.
- C. Training must be repeated frequently to respond to new legislation.
- D. Training must include assessments to verify that the material is mastered.

Answer: B

#### NEW QUESTION 178

##### 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.

To improve the facility's system of data security, Anton should consider following through with the plan for which of the following?

- A. Customer communication.
- B. Employee access to electronic storage.
- C. Employee advisement regarding legal matters.
- D. Controlled access at the company headquarters.

Answer: D

#### NEW QUESTION 179

Under the General Data Protection Regulation (GDPR), which of the following situations would LEAST likely require a controller to notify a data subject?

- A. An encrypted USB key with sensitive personal data is stolen
- B. A direct marketing email is sent with recipients visible in the 'cc' field
- C. Personal data of a group of individuals is erroneously sent to the wrong mailing list
- D. A hacker publishes usernames, phone numbers and purchase history online after a cyber-attack

Answer: B

#### NEW QUESTION 180

##### SCENARIO

Please use the following to answer the next QUESTION:

Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also

encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.

This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them."

Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!"

Which is the best first step in understanding the data security practices of a potential vendor?

- A. Requiring the vendor to complete a questionnaire assessing International Organization for Standardization (ISO) 27001 compliance.
- B. Conducting a physical audit of the vendor's facilities.
- C. Conducting a penetration test of the vendor's data security structure.
- D. Examining investigation records of any breaches the vendor has experienced.

**Answer: D**

### NEW QUESTION 183

#### SCENARIO

Please use the following to answer the next QUESTION:

John is the new privacy officer at the prestigious international law firm – A&M LLP. A&M LLP is very proud of its reputation in the practice areas of Trusts & Estates and Merger & Acquisition in both U.S. and Europe.

During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm's email continuity service to their existing email security vendor – MessageSafe. Being successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from Cloud Inc. to host email continuity service for A&M LLP.

John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe's previous breach and learned that the breach was caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.

At the meeting, Derrick emphasized that email is the primary method for the firm's lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn't have the time or resource to look for another solution. Furthermore, the off-premises email continuity service will only be turned on when the email service at A&M LLP's primary and secondary data centers are both down, and the email messages stored at MessageSafe site for continuity service will be automatically deleted after 30 days.

Which of the following is NOT an obligation of MessageSafe as the email continuity service provider for A&M LLP?

- A. Privacy compliance.
- B. Security commitment.
- C. Certifications to relevant frameworks.
- D. Data breach notification to A&M LLP.

**Answer: C**

### NEW QUESTION 188

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CIPM Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CIPM Product From:

<https://www.2passeasy.com/dumps/CIPM/>

## Money Back Guarantee

### CIPM Practice Exam Features:

- \* CIPM Questions and Answers Updated Frequently
- \* CIPM Practice Questions Verified by Expert Senior Certified Staff
- \* CIPM Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CIPM Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year