



CIPM^{Q&As}

Certified Information Privacy Manager

Pass IAPP CIPM Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/cipm.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

SCENARIO

Please use the following to answer the next QUESTION:

John is the new privacy officer at the prestigious international law firm AandM LLP. AandM LLP is very proud of its reputation in the practice areas of Trusts and Estates and Merger and 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 AandM 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 AandM 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. must notify AandM LLP of a data breach immediately.
- B. MessageSafe is liable if Cloud Inc. fails to protect data from AandM LLP.
- C. Cloud Inc. should enter into a data processor agreement with AandM LLP.
- D. AandM LLP's service contract must be amended to list Cloud Inc. as a sub-processor.

Correct Answer: A

QUESTION 2



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

- A. Failure to demonstrate that consent was given by the data subject to the processing of their personal data where it is used as the basis for processing
- B. Failure to implement technical and organizational measures to ensure data protection is enshrined by design and default
- C. Failure to process personal information in a manner compatible with its original purpose
- D. Failure to provide the means for a data subject to rectify inaccuracies in personal data

Correct Answer: A

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

QUESTION 3

When devising effective employee policies to address a particular issue, which of the following should be included in the first draft?

- A. Rationale for the policy.
- B. Points of contact for the employee.
- C. Roles and responsibilities of the different groups of individuals.
- D. of how the policy is applied within the organization.

Correct Answer: B

QUESTION 4

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.

Correct Answer: C

QUESTION 5

Which of the following indicates you have developed the right privacy framework for your organization?

- A. It includes a privacy assessment of each major system.
- B. It improves the consistency of the privacy program.
- C. It works at a different type of organization.
- D. It identifies all key stakeholders by name.

Correct Answer: A

QUESTION 6

As the Data Protection Officer (DPO) for the growing company, Vision 3468, what would be the most cost effective way to monitor changes in laws and regulations?

- A. Engage an external lawyer.
- B. Regularly engage regulators.
- C. Attend workshops and interact with other professionals.
- D. Subscribe to mailing lists that report on regulatory changes.

Correct Answer: D



QUESTION 7

What is most critical when outsourcing data destruction service?

- A. Obtain a certificate of data destruction.
- B. Confirm data destruction must be done on-site.
- C. Conduct an annual in-person audit of the provider's facilities.
- D. Ensure that they keep an asset inventory of the original data.

Correct Answer: D

QUESTION 8

SCENARIO

Please use the following to answer the next QUESTION:

You lead the privacy office for a company that handles information from individuals living in several countries throughout Europe and the Americas. You begin that morning's privacy review when a contracts officer sends you a message

asking for a phone call. The message lacks clarity and detail, but you presume that data was lost.

When you contact the contracts officer, he tells you that he received a letter in the mail from a vendor stating that the vendor improperly shared information about your customers. He called the vendor and confirmed that your company

recently surveyed exactly 2000 individuals about their most recent healthcare experience and sent those surveys to the vendor to transcribe it into a database, but the vendor forgot to encrypt the database as promised in the contract. As a

result, the vendor has lost control of the data.

The vendor is extremely apologetic and offers to take responsibility for sending out the notifications. They tell you they set aside 2000 stamped postcards because that should reduce the time it takes to get the notice in the mail. One side is

limited to their logo, but the other side is blank and they will accept whatever you want to write. You put their offer on hold and begin to develop the text around the space constraints. You are content to let the vendor's logo be associated with

the notification.

The notification explains that your company recently hired a vendor to store information about their most recent experience at St. Sebastian Hospital's Clinic for Infectious Diseases. The vendor did not encrypt the information and no longer

has control of it. All 2000 affected individuals are invited to sign-up for email notifications about their information. They simply need to go to your company's website and watch a quick advertisement, then provide their name, email address,

and month and year of birth.



You email the incident-response council for their buy-in before 9 a.m. If anything goes wrong in this situation, you want to diffuse the blame across your colleagues. Over the next eight hours, everyone emails their comments back and forth.

The consultant who leads the incident-response team notes that it is his first day with the company, but he has been in other industries for 45 years and will do his best. One of the three lawyers on the council causes the conversation to veer

off course, but it eventually gets back on track. At the end of the day, they vote to proceed with the notification you wrote and use the vendor's postcards.

Shortly after the vendor mails the postcards, you learn the data was on a server that was stolen, and make the decision to have your company offer credit monitoring services. A quick internet search finds a credit monitoring company with a

convincing name: Credit Under Lock and Key (CRUDLOK). Your sales rep has never handled a contract for 2000 people, but develops a proposal in about a day which says CRUDLOK will:

- 1.Send an enrollment invitation to everyone the day after the contract is signed.
- 2.Enroll someone with just their first name and the last-4 of their national identifier.
- 3.Monitor each enrollee's credit for two years from the date of enrollment.
- 4.Send a monthly email with their credit rating and offers for credit-related services at market rates.
- 5.Charge your company 20% of the cost of any credit restoration.

You execute the contract and the enrollment invitations are emailed to the 2000 individuals. Three days later you sit down and document all that went well and all that could have gone better. You put it in a file to reference the next time an

incident occurs.

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

- A. You convened it to diffuse blame
- B. The council has an overabundance of attorneys
- C. It takes eight hours of emails to come to a decision
- D. The leader just joined the company as a consultant

Correct Answer: A

QUESTION 9

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.

Knowing that the regulator is now investigating, what would be the best step to take?

- A. Consult an attorney experienced in privacy law and litigation.
- B. Use your background and knowledge to set a course of action.
- C. If you know the organization is guilty, advise it to accept the punishment.
- D. Negotiate the terms of a settlement before formal legal action takes place.

Correct Answer: A

QUESTION 10

Which of the following is NOT recommended for effective Identity Access Management?

- A. Demographics.
- B. Unique user IDs.
- C. User responsibility.
- D. Credentials (e.g., password).

Correct Answer: A

Explanation: Identity and Access Management (IAM) is a process that helps organizations secure their systems and data by controlling who has access to them and what they can do with that access. Effective IAM includes a number of best

practices, such as:

Unique user IDs: Each user should have a unique ID that is used to identify them across all systems and applications.

Credentials: Users should be required to provide authentication credentials, such as a password or biometric data, in



order to access systems and data. User responsibility: Users should be made aware of their responsibilities when it comes

to security, such as the need to keep their passwords secret and the importance of reporting suspicious activity.

Demographics refers to the statistical characteristics of a population, such as age, gender, income, etc. While demographic data may be collected and used for various purposes, it is not a recommended practice for effective IAM.

Demographic data is not a reliable method of identification or authentication, and it is not used to provide access to systems and data.

References:

<https://aws.amazon.com/iam/>

https://en.wikipedia.org/wiki/Identity_and_access_management <https://en.wikipedia.org/wiki/Demographics>

QUESTION 11

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.

Correct Answer: A

QUESTION 12

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.

Correct Answer: D

QUESTION 13

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.

Which of the following policy statements needs additional instructions in order to further protect the personal data of their clients?

- A. All faxes sent from the office must be documented and the phone number used must be double checked to ensure a safe arrival.
- B. All unused copies, prints, and faxes must be discarded in a designated recycling bin located near the work station and emptied daily.
- C. Before any copiers, printers, or fax machines are replaced or resold, the hard drives of these devices must be deleted before leaving the office.
- D. When sending a print job containing personal data, the user must not leave the information visible on the computer screen following the print command and must retrieve the printed document immediately.

Correct Answer: D

QUESTION 14

If your organization has a recurring issue with colleagues not reporting personal data breaches, all of the following are advisable to do EXCEPT?

- A. Review reporting activity on breaches to understand when incidents are being reported and when they are not to improve communication and training.
- B. Improve communication to reinforce to everyone that breaches must be reported and how they should be reported.
- C. Provide role-specific training to areas where breaches are happening so they are more aware.
- D. Distribute a phishing exercise to all employees to test their ability to recognize a threat attempt.

Correct Answer: D



Explanation: Distributing a phishing exercise is not advisable when attempting to address the issue of colleagues not reporting personal data breaches. Instead, the recommended steps are to review reporting activity on breaches, improve

communication, and provide role-specific training to areas where breaches are happening. These steps will help to ensure that everyone is aware of their responsibilities and that they understand how to report a breach should one occur.

References: <https://www.itgovernance.co.uk/blog/5-reasons-why-employees-dont-report-data-breaches/>

<https://www.ncsc.gov.uk/guidance/report-cyber-incident> <https://www.ncsc.gov.uk/guidance/phishing-staff-awareness>

QUESTION 15

SCENARIO

Please use the following to answer the next QUESTION:

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

Correct Answer: A

[CIPM PDF Dumps](#)

[CIPM Practice Test](#)

[CIPM Exam Questions](#)