Vendor:IAPP

Exam Code:CIPM

Exam Name: Certified Information Privacy Manager

Version: Demo

QUESTION 1

Internal audits add value to the privacy program primarily though what?

A. Evaluating the effectiveness of the privacy program.

B. Remediating gaps in the privacy program noted by management.

C. Remediating gaps in the privacy program noted within audit reports.

D. Determining the applicability of certain privacy regulations to the organization.

Correct Answer: A

QUESTION 2

Which of the following information must be provided by the data controller when complying with GDPR "right to be informed" requirements?

A. The purpose of personal data processing.

B. The data subject\\'s right to withdraw consent

C. The contact details of the Data Protection Officer (DPO).

D. The name of any organizations with whom personal data was shared.

Correct Answer: C

QUESTION 3

SCENARIO

Please use the following to answer the next question:

Felicity is the Chief Executive Officer (CEO) of an international clothing company that does business in several countries, including the United States (U.S.), the United Kingdom (UK), and Canada. For the first five years under Felicity\\'s

leadership, the company was highly successful due its higher profile on the Internet via target advertising and the use of social media. However, business has dropped in recent months, and Felicity is looking to cut costs across all

departments.

She has prepared to meet with the Chief Information Officer (CIO), Jin, who is also head of the company\\'s privacy program.

After reviewing many of Jin\\'s decisions, Felicity firmly believes that, although well-intentioned, Jin overspends company resources. Felicity has taken several notes on ways she believes the company can spend less money trying to

uphold its

privacy mission. First, Felicity intends to discuss the size of the company\\'s information security budget with Jin. Felicity proposes to streamline information security by putting it solely within the purview of the company\\'s Information Technology

(IT) experts, since personal data within the company is stored electronically.

She is also perplexed by the Privacy Impact Assessments (PIAs) Jin facilitated at some of the company\\'s locations. Jin carefully documented the approximate amount of man-hours the PIAs took to complete, and Felicity is astounded at the

amount. She cannot understand why so much time has been spent on sporadic PIAs.

Felicity has also recently received complaints from employees, including mid-level managers, about the great burden of paperwork necessary for documenting employee compliance with the company\\'s privacy policy. She hopes Jin can

propose cheaper, more efficient ways of monitoring compliance. In Felicity\\'s view, further evidence of Jin\\'s overzealousness is his insistence on monitoring third-party processors for their observance of the company\\'s privacy policy. New staff

members seem especially overwhelmed. Despite the consistent monitoring, two years ago the company had to pay remediation costs after a security breach of a processor\\'s data system. Felicity wonders whether processors can be held

contractually liable for the costs of any future breaches.

Last in Felicity\\'s notes is a reminder to discuss Jin\\'s previous praise for the company\\'s independent ethics function within the Human Resources (HR) department. Felicity believes that much company time could be saved if the Ethics Officer

position were done away with, and that any ethical concerns were simply brought directly to the executive leadership of the company.

Although Felicity questions many of Jin\\'s decisions, she hopes that their meeting will be productive and that Jin, who is widely respected throughout the company, will help the company save money. Felicity believes that austerity is the only

way forward.

Based on the scenario, Felicity is in danger of NOT exercising enough caution regarding?

A. The company\\'s acceptance of advanced technology.

B. The company\\'s ongoing relationship with outside vendors.

C. The allocation of duties to a Chief Information Officer (CIO).

D. The staff charged with assisting with Privacy Impact Assessments (PIAs).

Correct Answer: C

QUESTION 4

SCENARIO

Please use the following to answer the next QUESTION:

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

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

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

following day, to get insight into how the office computer system is currently set-up and managed.

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.

Correct Answer: A

QUESTION 5

The least useful metric for optimizing the design of your data subject request workflow is tracking the number of data subjects who?

A. Made requests by geographic origin.

B. Used an automated service for the request.

C. Made requests to know vs. requests to be deleted.

D. Authorized another person to make the request on their behalf.

Correct Answer: B

QUESTION 6

Which of the following best describes proper compliance for an international organization using Binding Corporate Rules (BCRs) as a controller or processor?

A. Employees must sign an ad hoc contractual agreement each time personal data is exported.

B. All employees are subject to the rules in their entirety, regardless of where the work is taking place.

C. All employees must follow the privacy regulations of the jurisdictions where the current scope of their work is established.

D. Employees who control personal data must complete a rigorous certification procedure, as they are exempt from legal enforcement.

Correct Answer: A

Reference: https://www.lexology.com/library/detail.aspx?g=80239951-01b8-409f-9019- 953f5233852e

---

QUESTION 7

SCENARIO

Please use the following to answer the next QUESTION:

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

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

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

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

Correct Answer: C

QUESTION 8

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 9

What should be the first major goal of a company developing a new privacy program?

A. To survey potential funding sources for privacy team resources.

B. To schedule conversations with executives of affected departments.

C. To identify potential third-party processors of the organization\\'s information.

D. To create Data Lifecycle Management policies and procedures to limit data collection.

Correct Answer: D

QUESTION 10

Which of the following actions is NOT required during a data privacy diligence process for Merger and Acquisition (MandA) deals?

A. Revise inventory of applications that house personal data and data mapping.

B. Update business processes to handle Data Subject Requests (DSRs).

C. Compare the original use of personal data to post-merger use.

D. Perform a privacy readiness assessment before the deal.

Correct Answer: D

QUESTION 11

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

Correct Answer: A

QUESTION 12

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.

Correct Answer: C