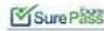


CIPM Actual Tests & CIPM Answers Free



Recommend!! Get the Full CIPM dumps in VCE and PDF From SurePassExam
<https://www.surepassexam.com/CIPM-exam-dumps.html> (159 New Questions)

IAPP

Exam Questions CIPM

Certified Information Privacy Manager (CIPM)



Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

BTW, DOWNLOAD part of PrepAwayExam CIPM dumps from Cloud Storage: <https://drive.google.com/open?id=1oPh8qfG2CZPoS5elqGDHGQecvVx8z8Mj>

To keep you updated with latest changes in the CIPM test questions, we offer one-year free updates in the form of new questions according to the requirement of CIPM real exam. Updated CIPM vce dumps ensure the accuracy of learning materials and guarantee success of in your first attempt. Why not let our CIPM Dumps Torrent help you to pass your exam without spending huge amount of money.

IAPP CIPM (Certified Information Privacy Manager) certification exam is a globally recognized certification that validates the knowledge and skills of privacy professionals in managing and implementing privacy programs. Certified Information Privacy Manager (CIPM) certification is designed for professionals who are responsible for managing and overseeing privacy programs within their organization. CIPM exam covers a broad range of topics, including privacy program governance, privacy policies and procedures, privacy training and awareness, data protection and management, and privacy incident management.

IAPP CIPM Exam is designed for professionals who are responsible for managing privacy programs, including privacy officers, data protection officers, information security officers, and compliance officers. CIPM exam tests the knowledge and skills of the candidates in privacy program management, privacy operations, and privacy regulations. CIPM Exam is a comprehensive assessment of the candidate's ability to manage privacy programs and ensure compliance with privacy regulations.

The CIPM exam covers a broad range of topics related to privacy management, including privacy program governance, privacy program operationalization, privacy program assessment, and privacy program communication. CIPM exam also covers the legal and regulatory frameworks related to privacy, such as GDPR, CCPA, and HIPAA. The CIPM exam is designed for professionals with at least two years of experience in privacy management or a related field. CIPM exam consists of 90 multiple-choice questions and must be completed within two hours.

Unparalleled CIPM Actual Tests | Easy To Study and Pass Exam at first attempt & Trustable IAPP Certified Information Privacy Manager (CIPM)

As is known to us, our company is professional brand established for compiling the CIPM exam materials for all candidates. The CIPM guide files from our company are designed by a lot of experts and professors of our company in the field. We can promise that the CIPM certification braindumps of our company have the absolute authority in the study materials market. We believe that the study materials designed by our company will be the most suitable choice for you. You can totally depend on the CIPM Guide files of our company when you are preparing for the exam.

IAPP Certified Information Privacy Manager (CIPM) Sample Questions (Q66-Q71):

NEW QUESTION # 66

How do privacy audits differ from privacy assessments?

- A. They are non-binding.
- B. They are conducted by external parties.
- C. They are evidence-based.
- D. They are based on standards.

Answer: C

Explanation:

Privacy audits differ from privacy assessments in that they are evidence-based, meaning that they rely on objective and verifiable data to evaluate the compliance and effectiveness of the privacy program. Privacy assessments, on the other hand, are based on standards, meaning that they use a set of criteria or best practices to measure the performance and maturity of the privacy program. Privacy audits are usually conducted by external parties, while privacy assessments can be done internally or externally. Reference: CIPM Body of Knowledge, Domain III: Privacy Program Operational Life Cycle, Section A: Assess, Subsection 1: Privacy Assessments and Audits.

NEW QUESTION # 67

What is the function of the privacy operational life cycle?

- A. It ensures that outdated privacy policies are retired on a set schedule
- B. It allows privacy policies to mature to a fixed form
- C. It allows the organization to respond to ever-changing privacy demands
- D. It establishes initial plans for privacy protection and implementation

Answer: D

NEW QUESTION # 68

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 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.

Based on the scenario, Nationwide Grill needs to create better employee awareness of the company's privacy program by doing what?

- A. Communicating to the staff more often.
- B. Improving inter-departmental cooperation.
- C. Requiring acknowledgment of company memos.
- D. Varying the modes of communication.

Answer: C

NEW QUESTION # 69

What is the function of the privacy operational life cycle?

- A. It ensures that outdated privacy policies are retired on a set schedule
- B. It allows the organization to respond to ever-changing privacy demands
- C. It allows privacy policies to mature to a fixed form
- D. It establishes initial plans for privacy protection and implementation

Answer: B

Explanation:

The privacy operational life cycle is a process that allows the organization to respond to ever-changing privacy demands by continuously monitoring and improving the privacy program. It consists of four phases: assess, protect, sustain, and respond. Each phase involves different activities and outputs that help the organization identify and manage privacy risks and opportunities. References: IAPP CIPM Study Guide, page 14.

NEW QUESTION # 70

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?

