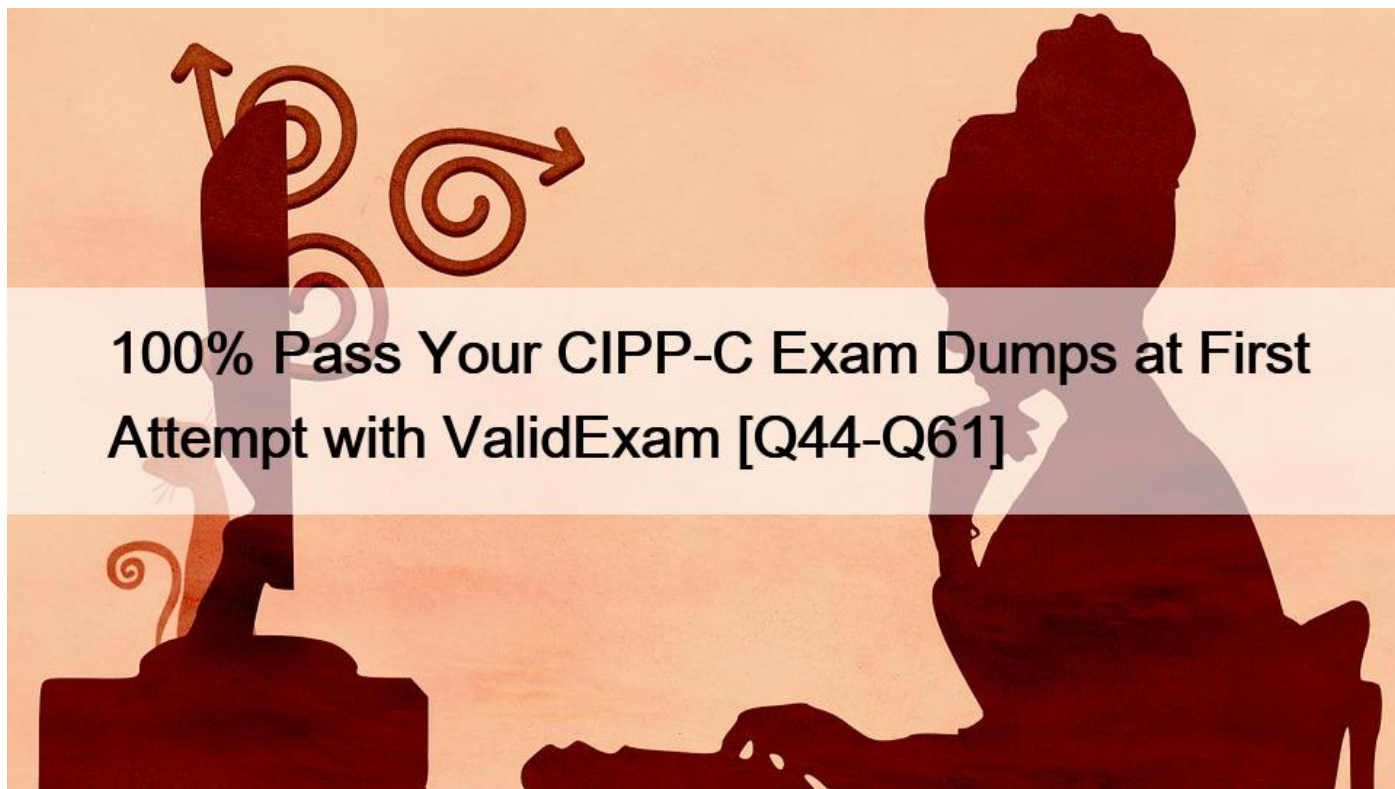


100% Pass Your CIPP-C Exam Dumps at First Attempt with ValidExam [Q44-Q61]



100% Pass Your CIPP-C Exam Dumps at First Attempt with ValidExam
Penetration testers simulate CIPP-C exam PDF

Difficulty in writing IAPP CIPP-C Certification Exam:

Difficulties in writing this exam are you have to know a lot about information protection and privacy law, regulation, and standards. That means you have to do a lot of homework and reading. The process of writing the CIPP-C exam is not as difficult as you think. IAPP provides a wide range of materials to prepare for the exam. The consumer can access all the information for free for your reference on the IAPP website. Busy schedules and financial problems can be overcome by taking free online IAPP CIPP-C quizzes. Simulator tests are designed to check your knowledge about the subject. They are available on the IAPP website for free as well as the IAPP CIPP-C book. All these materials can help you to be ready for the exam.

The study guide covers all of the topics you will encounter on your exam, so it is really good to know what topics are covered on the practice test before you take the actual exam. Undecided about the IAPP CIPP-C exam? You can take a practice test by using **IAPP CIPP-C exam dumps** and check out your performance. Consultation with the IAPP CIPP-C certified trainer is recommended to help you pass the exam. Products like the CIPP-C book are also really helpful to enhance your knowledge. Programs like the CIPP-C boot camps are also designed to provide you with support. A chance of success is obtained if you apply the study guide to the test questions. Excellent resource material is important to obtain the certification IAPP CIPP-C.

What is the Passing Score, Duration & Questions for the IAPP CIPP-C Exam

The passing score is 75 percent. The duration of the IAPP CIPP-C certification exam is 2 hours. The questions are objective type. There are 100 questions in total on the IAPP CIPP-C exam. IAPP real cpractice test questions are available to certify the candidate's knowledge of the subject by testing on actual exam topics. Apps for smartphones and tablets are also provided to ensure easy and

quick access to the fastest material.

Q44. SCENARIO

Looking back at your first two years as the Director of Personal Information Protection and Compliance for the Berry Country Regional Medical Center in Thorn Bay, Ontario, Canada, you see a parade of accomplishments, from developing state-of-the-art simulation based training for employees on privacy protection to establishing an interactive medical records system that is accessible by patients as well as by the medical personnel. Now, however, a question you have put off looms large: how do we manage all the data-not only records produced recently, but those still on hand from years ago? A data flow diagram generated last year shows multiple servers, databases, and work stations, many of which hold files that have not yet been incorporated into the new records system. While most of this data is encrypted, its persistence may pose security and compliance concerns. The situation is further complicated by several long-term studies being conducted by the medical staff using patient information. Having recently reviewed the major Canadian privacy regulations, you want to make certain that the medical center is observing them.

You also recall a recent visit to the Records Storage Section, often termed *'The Dungeon'*; in the basement of the old hospital next to the modern facility, where you noticed a multitude of paper records. Some of these were in crates marked by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. The back shelves of the section housed data tapes and old hard drives that were often unlabeled but appeared to be years old. On your way out of the dungeon, you noticed just ahead of you a small man in a lab coat who you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.

Which cryptographic standard would be most appropriate for protecting patient credit card information in the records system?

- * Asymmetric Encryption
- * Symmetric Encryption
- * Obfuscation
- * Hashing

Q45. All of the following common law torts are relevant to employee privacy under US law EXCEPT?

- * Infliction of emotional distress.
- * Intrusion upon seclusion.
- * Defamation
- * Conversion.

Q46. SCENARIO

Please use the following to answer the next QUESTION:

You are the chief privacy officer at HealthCo, a major hospital in a large U.S. city in state A.

HealthCo is a HIPAA-covered entity that provides healthcare services to more than 100,000 patients. A third-party cloud computing service provider, CloudHealth, stores and manages the electronic protected health information (ePHI) of these individuals on behalf of HealthCo. CloudHealth stores the data in state B.

As part of HealthCo's business associate agreement (BAA) with CloudHealth, HealthCo requires CloudHealth to implement security measures, including industry standard encryption practices, to adequately protect the data. However, HealthCo did not perform due diligence on CloudHealth before entering the contract, and has not conducted audits of CloudHealth's security measures. A CloudHealth employee has recently become the victim of a phishing attack. When the employee unintentionally clicked on a link from a suspicious email, the PHI of more than 10,000 HealthCo patients was compromised. It has since been published online. The HealthCo cybersecurity team quickly identifies the perpetrator as a known hacker who has launched similar attacks on

other hospitals; ones that exposed the PHI of public figures including celebrities and politicians.

During the course of its investigation, HealthCo discovers that CloudHealth has not encrypted the PHI in accordance with the terms of its contract. In addition, CloudHealth has not provided privacy or security training to its employees. Law enforcement has requested that HealthCo provide its investigative report of the breach and a copy of the PHI of the individuals affected.

A patient affected by the breach then sues HealthCo, claiming that the company did not adequately protect the individual's ePHI, and that he has suffered substantial harm as a result of the exposed data. The patient's attorney has submitted a discovery request for the ePHI exposed in the breach.

What is the most effective kind of training CloudHealth could have given its employees to help prevent this type of data breach?

- * Training on techniques for identifying phishing attempts
- * Training on the terms of the contractual agreement with HealthCo
- * Training on the difference between confidential and non-public information
- * Training on CloudHealth's HR policy regarding the role of employees involved data breaches

Q47. Under the GDPR, which essential pieces of information must be provided to data subjects before collecting their personal data?

- * The authority by which the controller is collecting the data and the third parties to whom the data will be sent.
- * The name/s of relevant government agencies involved and the steps needed for revising the data.
- * The identity and contact details of the controller and the reasons the data is being collected.
- * The contact information of the controller and a description of the retention policy.

Q48. Which EU institution is vested with the competence to propose new data protection legislation on its own initiative?

- * The Canadian Council
- * The Canadian Parliament
- * The Canadian Commission
- * Office of the Privacy Commissioner of Canada

Q49. What do the Civil Rights Act, Pregnancy Discrimination Act, Americans with Disabilities Act, Age Discrimination Act, and Equal Pay Act all have in common?

- * They require employers not to discriminate against certain classes when employees use personal information
- * They require that employers provide reasonable accommodations to certain classes of employees
- * They afford certain classes of employees' privacy protection by limiting inquiries concerning their personal information
- * They permit employers to use or disclose personal information specifically about employees who are members of certain classes

Q50. Which action is prohibited under the Electronic Communications Privacy Act of 1986?

- * Intercepting electronic communications and unauthorized access to stored communications
- * Monitoring all employee telephone calls
- * Accessing stored communications with the consent of the sender or recipient of the message
- * Monitoring employee telephone calls of a personal nature

Q51. In 2012, the White House and the FTC both issued reports advocating a new approach to privacy enforcement that can best be described as what?

- * Harm-based.
- * Self-regulatory.
- * Comprehensive.
- * Notice and choice.

Q52. SCENARIO

Please use the following to answer the next QUESTION

Felicia has spent much of her adult life overseas, and has just recently returned to the U.S. to help her friend Celeste open a jewelry store in California. Felicia, despite being excited at the prospect, has a number of security concerns, and has only grudgingly accepted the need to hire other employees. In order to guard against the loss of valuable merchandise, Felicia wants to carefully screen applicants. With their permission, Felicia would like to run credit checks, administer polygraph tests, and scrutinize videos of interviews. She intends to read applicants' postings on social media, ask questions about drug addiction, and solicit character references. Felicia believes that if potential employees are serious about becoming part of a dynamic new business, they will readily agree to these requirements.

Felicia is also in favor of strict employee oversight. In addition to protecting the inventory, she wants to prevent mistakes during transactions, which will require video monitoring. She also wants to regularly check the company vehicle's GPS for locations visited by employees. She also believes that employees who use their own devices for work-related purposes should agree to a certain amount of supervision.

Given her high standards, Felicia is skeptical about the proposed location of the store. She has been told that many types of background checks are not allowed under California law. Her friend Celeste thinks these worries are unfounded, as long as applicants verbally agree to the checks and are offered access to the results. Nor does Celeste share Felicia's concern about state breach notification laws, which, she claims, would be costly to implement even on a minor scale. Celeste believes that even if the business grows a customer database of a few thousand, it's unlikely that a state agency would hassle an honest business if an accidental security incident were to occur.

In any case, Celeste feels that all they need is common sense - like remembering to tear up sensitive documents before throwing them in the recycling bin. Felicia hopes that she's right, and that all of her concerns will be put to rest next month when their new business consultant (who is also a privacy professional) arrives from North Carolina.

Regarding credit checks of potential employees, Celeste has a misconception regarding what?

- * Consent requirements.
- * Disclosure requirements.
- * Employment-at-will rules.
- * Records retention policies

Q53. When does the Telemarketing Sales Rule require an entity to share a do-not-call request across its organization?

- * When the operational structures of its divisions are not transparent
- * When the goods and services sold by its divisions are very similar
- * When a call is not the result of an error or other unforeseen cause
- * When the entity manages user preferences through multiple platforms

Q54. Which of the following became the first state to pass a law specifically regulating the practices of data brokers?

- * Washington.
- * California.
- * New York.
- * Vermont.

Q55. What is true if an employee makes an access request to his employer for any personal data held about him?

- * The employer can automatically decline the request if it contains personal data about a third person.
- * The employer can decline the request if the information is only held electronically.
- * The employer must supply all the information held about the employee.
- * The employer must supply any information held about an employee unless an exemption applies.

Q56. As a result of the European Court of Justice's ruling in the case of Google v. Spain, search engines outside the EEA are also likely to be subject to the Regulation's right to be forgotten. This holds true if the activities of an EU subsidiary and its U.S. parent are what?

- * Supervised by the same Data Protection Officer.
- * Consistent with Privacy Shield requirements
- * Bound by a standard contractual clause.
- * Inextricably linked in their businesses.

Q57. What is the MAIN reason GDPR Article 4(22) establishes the concept of the concerned supervisory authority?

- * To encourage the consistency of local data processing activity.
- * To give corporations a choice about who their supervisory authority will be.
- * To ensure the GDPR covers controllers that do not have an establishment in the EU but have a representative in a member state.
- * To ensure that the interests of individuals residing outside the lead authority's jurisdiction are represented.

Q58. SCENARIO

Please use the following to answer the next question:

Brady is a computer programmer based in New Zealand who has been running his own business for two years.

Brady's business provides a low-cost suite of services to customers throughout the European Economic Area (EEA). The services are targeted towards new and aspiring small business owners. Brady's company, called Brady Box, provides web page design services, a Social Networking Service (SNS) and consulting services that help people manage their own online stores.

Unfortunately, Brady has been receiving some complaints. A customer named Anna recently uploaded her plans for a new product onto Brady Box's chat area, which is open to public viewing. Although she realized her mistake two weeks later and removed the document, Anna is holding Brady Box responsible for not noticing the error through regular monitoring of the website. Brady believes he should not be held liable.

Another customer, Felipe, was alarmed to discover that his personal information was transferred to a third-party contractor called Hermes Designs and worries that sensitive information regarding his business plans may be misused. Brady does not believe he violated European privacy rules. He provides a privacy notice to all of his customers explicitly stating that personal data may be transferred to specific third parties in fulfillment of a requested service. Felipe says he read the privacy notice but that it was long and complicated. Brady continues to insist that Felipe has no need to be concerned, as he can personally vouch for the integrity of Hermes Designs. In fact, Hermes Designs has taken the initiative to create sample customized banner advertisements for customers like Felipe. Brady is happy to provide a link to the example banner ads, now posted on the Hermes Designs webpage. Hermes Designs plans on following up with direct marketing to these customers.

Brady was surprised when another customer, Serge, expressed his dismay that a quotation by him is being used within a graphic collage on Brady Box's home webpage. The quotation is attributed to Serge by first and last name. Brady, however, was not worried about any sort of litigation. He wrote back to Serge to let him know that he found the quotation within Brady Box's Social Networking Service (SNS), as Serge himself had posted the quotation. In his response, Brady did offer to remove the quotation as a courtesy.

Despite some customer complaints, Brady's business is flourishing. He even supplements his income through online behavioral advertising (OBA) via a third-party ad network with whom he has set clearly defined roles.

Brady is pleased that, although some customers are not explicitly aware of the OBA, the advertisements contain useful products and

services.

Based on the scenario, what is the main reason that Brady should be concerned with Hermes Designs' handling of customer personal data?

- * The data is sensitive.
- * The data is uncategorized.
- * The data is being used for a new purpose.
- * The data is being processed via a new means.

Q59. Which entity within the Department of Health and Human Services (HHS) is the primary enforcer of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule?

- * Office for Civil Rights.
- * Office of Social Services.
- * Office of Inspector General.
- * Office of Public Health and Safety.

Q60. WP29's Guidelines on Personal data breach notification under Regulation 2016/679 provides examples of ways to communicate data breaches transparently. Which of the following was listed as a method that would NOT be effective for communicating a breach to data subjects?

- * A postal notification
- * A direct electronic message
- * A notice on a corporate blog
- * A prominent advertisement in print media

Q61. Which of the following would NOT be relevant when determining if a processing activity would be considered profiling?

- * If the processing is to be performed by a third-party vendor
- * If the processing involves data that is considered personal data
- * If the processing of the data is done through automated means
- * If the processing is used to predict the behavior of data subjects

All CIPP-C Dumps and Training Courses: <https://www.validexam.com/CIPP-C-latest-dumps.html>