



**IAPP**

**Exam Questions CIPT**

Certified Information Privacy Technologist

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

#### SCENARIO

Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database - currently managed in-house by Clean-Q IT Support. Because of Clean-Q's business model, resources are contracted as needed instead of permanently employed.

The table below indicates some of the personal information Clean-Q requires as part of its business operations:

Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario. With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q's traditional supply and demand system that has caused some overlapping bookings.

In a business strategy session held by senior management recently, Clean-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q's solution providers, presenting their proposed solutions and platforms.

The Managing Director opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.

- A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
- A resource facing web interface that enables resources to apply and manage their assigned jobs.
- An online payment facility for customers to pay for services.

Which question would you most likely ask to gain more insight about LeadOps and provide practical privacy recommendations?

- A. What is LeadOps' annual turnover?
- B. How big is LeadOps' employee base?
- C. Where are LeadOps' operations and hosting services located?
- D. Does LeadOps practice agile development and maintenance of their system?

**Answer: D**

### NEW QUESTION 2

Which is the most accurate type of biometrics?

- A. DNA
- B. Voiceprint.
- C. Fingerprint.
- D. Facial recognition.

**Answer: B**

### NEW QUESTION 3

What risk is mitigated when routing video traffic through a company's application servers, rather than sending the video traffic directly from one user to another?

- A. The user is protected against phishing attacks.
- B. The user's identity is protected from the other user.
- C. The user's approximate physical location is hidden from the other user.
- D. The user is assured that stronger authentication methods have been used.

**Answer: B**

### NEW QUESTION 4

Properly configured databases and well-written website codes are the best protection against what online threat?

- A. Pharming.
- B. SQL injection.
- C. Malware execution.
- D. System modification.

**Answer: B**

### NEW QUESTION 5

What can be used to determine the type of data in storage without exposing its contents?

- A. Collection records.
- B. Data mapping.
- C. Server logs.
- D. Metadata.

**Answer: D**

#### NEW QUESTION 6

How can a hacker gain control of a smartphone to perform remote audio and video surveillance?

- A. By performing cross-site scripting.
- B. By installing a roving bug on the phone.
- C. By manipulating geographic information systems.
- D. By accessing a phone's global positioning system satellite signal.

**Answer: B**

#### NEW QUESTION 7

What tactic does pharming use to achieve its goal?

- A. It modifies the user's Hosts file.
- B. It encrypts files on a user's computer.
- C. It creates a false display advertisement.
- D. It generates a malicious instant message.

**Answer: C**

#### NEW QUESTION 8

Under the Family Educational Rights and Privacy Act (FERPA), releasing personally identifiable information from a student's educational record requires written permission from the parent or eligible student in order for information to be?

- A. Released to a prospective employer.
- B. Released to schools to which a student is transferring.
- C. Released to specific individuals for audit or evaluation purposes.
- D. Released in response to a judicial order or lawfully ordered subpoena.

**Answer: C**

#### NEW QUESTION 9

##### SCENARIO

Please use the following to answer the next question:

Light Blue Health (LBH) is a healthcare technology company developing a new web and mobile application that collects personal health information from electronic patient health records. The application will use machine learning to recommend potential medical treatments and medications based on information collected from anonymized electronic health records. Patient users may also share health data collected from other mobile apps with the LBH app.

The application requires consent from the patient before importing electronic health records into the application and sharing it with their authorized physicians or healthcare provider. The patient can then review and share the recommended treatments with their physicians securely through the app. The patient user may also share location data and upload photos in the app. The patient user may also share location data and upload photos in the app for a healthcare provider to review along with the health record. The patient may also delegate access to the app.

LBH's privacy team meets with the Application development and Security teams, as well as key business stakeholders on a periodic basis. LBH also implements Privacy by Design (PbD) into the application development process.

The Privacy Team is conducting a Privacy Impact Assessment (PIA) to evaluate privacy risks during development of the application. The team must assess whether the application is collecting descriptive, demographic or any other user related data from the electronic health records that are not needed for the purposes of the application. The team is also reviewing whether the application may collect additional personal data for purposes for which the user did not provide consent.

What is the best way to ensure that the application only collects personal data that is needed to fulfill its primary purpose of providing potential medical and healthcare recommendations?

- A. Obtain consent before using personal health information for data analytics purposes.
- B. Provide the user with an option to select which personal data the application may collect.
- C. Disclose what personal data the application is collecting in the company Privacy Policy posted online.
- D. Document each personal category collected by the app and ensure it maps to an app function or feature.

**Answer: C**

#### NEW QUESTION 10

In order to prevent others from identifying an individual within a data set, privacy engineers use a cryptographically-secure hashing algorithm. Use of hashes in this way illustrates the privacy tactic known as what?

- A. Isolation.
- B. Obfuscation.
- C. Perturbation.
- D. Stripping.

**Answer: B**

#### NEW QUESTION 10

What is the goal of privacy enhancing technologies (PETs) like multiparty computation and differential privacy?

- A. To facilitate audits of third party vendors.
- B. To protect sensitive data while maintaining its utility.
- C. To standardize privacy activities across organizational groups.
- D. To protect the security perimeter and the data items themselves.

**Answer: B**

#### NEW QUESTION 14

##### SCENARIO

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving. However, the company now sells online through retail sites designated for industries and demographics, sites such as "My Cool Ride" for automobile-related products or "Zoomer" for gear aimed toward young adults. The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.

You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company's culture. For this project, you are considering using a series of third-party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company's product lines as well as products from affiliates. This new omnibus site will be known, aptly, as "Under the Sun." The Director of Marketing wants the site not only to sell Ancillary's products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

Which should be used to allow the home sales force to accept payments using smartphones?

- A. Field transfer protocol.
- B. Cross-current translation.
- C. Near-field communication
- D. Radio Frequency Identification

**Answer: C**

#### NEW QUESTION 15

##### SCENARIO

Please use the following to answer the next question:

Looking back at your first two years as the Director of Personal Information Protection and Compliance for the St. Anne's 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 recall a recent visit to the Records Storage Section in the basement of the old hospital next to the modern facility, where you noticed paper records sitting in crates labeled by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. On the back shelves of the section sat data tapes and old hard drives that were often unlabeled but appeared to be years old. On your way out of the records storage section, you noticed a man leaving whom you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.

You quickly realize that you need a plan of action on the maintenance, secure storage and disposal of data. Which cryptographic standard would be most appropriate for protecting patient credit card information in the records system at St. Anne's Regional Medical Center?

- A. Symmetric Encryption
- B. Tokenization
- C. Obfuscation
- D. Certificates

**Answer: B**

#### NEW QUESTION 19

What must be used in conjunction with disk encryption?

- A. Increased CPU speed.
- B. A strong password.
- C. A digital signature.
- D. Export controls.

**Answer: C**

#### NEW QUESTION 20

Value Sensitive Design (VSD) focuses on which of the following?

- A. Quality and benefit.
- B. Ethics and morality.
- C. Principles and standards.
- D. Privacy and human rights.

**Answer: C**

#### NEW QUESTION 22

To comply with the Sarbanes-Oxley Act (SOX), public companies in the United States are required to annually report on the effectiveness of the auditing controls of their financial reporting systems. These controls must be implemented to prevent unauthorized use, disclosure, modification, and damage or loss of financial data.

Why do these controls ensure both the privacy and security of data?

- A. Modification of data is an aspect of privacy; unauthorized use, disclosure, and damage or loss of data are aspects of security.
- B. Unauthorized use of data is an aspect of privacy; disclosure, modification, and damage or loss of data are aspects of security.
- C. Disclosure of data is an aspect of privacy; unauthorized use, modification, and damage or loss of data are aspects of security.
- D. Damage or loss of data are aspects of privacy; disclosure, unauthorized use, and modification of data are aspects of privacy.

**Answer: C**

#### NEW QUESTION 24

What is the potential advantage of homomorphic encryption?

- A. Encrypted information can be analyzed without decrypting it first.
- B. Ciphertext size decreases as the security level increases.
- C. It allows greater security and faster processing times.
- D. It makes data impenetrable to attacks.

**Answer: C**

#### NEW QUESTION 28

##### SCENARIO

WebTracker Limited is a cloud-based online marketing service located in London. Last year, WebTracker migrated its IT infrastructure to the cloud provider Azure, which provides SQL Databases and Artificial Intelligence services to WebTracker. The roles and responsibilities between the two companies have been formalized in a standard contract, which includes allocating the role of data controller to WebTracker.

The CEO of WebTracker, Mr. Bond, would like to assess the effectiveness of Azure's privacy controls, and he recently decided to hire you as an independent auditor. The scope of the engagement is limited only to the marketing services provided by WebTracker, you will not be evaluating any internal data processing activity, such as HR or Payroll.

This ad-hoc audit was triggered due to a future partnership between WebTracker and SmartHome — a partnership that will not require any data sharing.

SmartHome is based in the USA, and most recently has dedicated substantial resources to developing smart refrigerators that can suggest the recommended daily calorie intake based on DNA information. This and other personal data is collected by WebTracker.

To get an idea of the scope of work involved, you have decided to start reviewing the company's documentation and interviewing key staff to understand potential privacy risks.

The results of this initial work include the following notes:

- There are several typos in the current privacy notice of WebTracker, and you were not able to find the privacy notice for SmartHome.
- You were unable to identify all the sub-processors working for SmartHome. No subcontractor is indicated in the cloud agreement with Azure, which is responsible for the support and maintenance of the cloud infrastructure.
- There are data flows representing personal data being collected from the internal employees of WebTracker, including an interface from the HR system.
- Part of the DNA data collected by WebTracker was from employees, as this was a prototype approved by the CEO of WebTracker.
- All the WebTracker and SmartHome customers are based in USA and Canada.

Based on the initial assessment and review of the available data flows, which of the following would be the most important privacy risk you should investigate first?

- A. Verify that WebTracker's HR and Payroll systems implement the current privacy notice (after the typos are fixed).
- B. Review the list of subcontractors employed by Azure and ensure these are included in the formal agreement with WebTracker.
- C. Evaluate and review the basis for processing employees' personal data in the context of the prototype created by WebTracker and approved by the CEO.
- D. Confirm whether the data transfer from London to the USA has been fully approved by Azure and the appropriate institutions in the USA and the European Union.

**Answer: C**

#### NEW QUESTION 31

##### SCENARIO

Please use the following to answer the next question:

Jordan just joined a fitness-tracker start-up based in California, USA, as its first Information Privacy and Security Officer. The company is quickly growing its business but does not sell any of the fitness trackers itself. Instead, it relies on a distribution network of third-party retailers in all major countries. Despite not having any stores, the company has a 78% market share in the EU. It has a website presenting the company and products, and a member section where customers can access their information. Only the email address and physical address need to be provided as part of the registration process in order to customize the site to the user's region and country. There is also a newsletter sent every month to all members featuring fitness tips, nutrition advice, product spotlights from partner companies based on user behavior and preferences.

Jordan says the General Data Protection Regulation (GDPR) does not apply to the company. He says the company is not established in the EU, nor does it have a processor in the region. Furthermore, it does not do any "offering goods or services" in the EU since it does not do any marketing there, nor sell to consumers directly. Jordan argues that it is the customers who chose to buy the products on their own initiative and there is no "offering" from the company.

The fitness trackers incorporate advanced features such as sleep tracking, GPS tracking, heart rate monitoring, wireless syncing, calorie-counting and step-tracking. The watch must be paired with either a smartphone or a computer in order to collect data on sleep levels, heart rates, etc. All information from the device must be sent to the company's servers in order to be processed, and then the results are sent to the smartphone or computer. Jordan argues that there is no personal information involved since the company does not collect banking or social security information.

Based on the current features of the fitness watch, what would you recommend be implemented into each device in order to most effectively ensure privacy?

- A. Hashing.
- B. A2DP Bluetooth profile.
- C. Persistent unique identifier.
- D. Randomized MAC address.

**Answer: C**

#### NEW QUESTION 36

Which of the following most embodies the principle of Data Protection by Default?

- A. A messaging app for high school students that uses HTTPS to communicate with the server.
- B. An electronic teddy bear with built-in voice recognition that only responds to its owner's voice.
- C. An internet forum for victims of domestic violence that allows anonymous posts without registration.
- D. A website that has an opt-in form for marketing emails when registering to download a whitepaper.

**Answer:** D

#### NEW QUESTION 38

What privacy risk is NOT mitigated by the use of encrypted computation to target and serve online ads?

- A. The ad being served to the user may not be relevant.
- B. The user's sensitive personal information is used to display targeted ads.
- C. The personal information used to target ads can be discerned by the server.
- D. The user's information can be leaked to an advertiser through weak de-identification techniques.

**Answer:** D

#### NEW QUESTION 42

What is typically NOT performed by sophisticated Access Management (AM) techniques?

- A. Restricting access to data based on location.
- B. Restricting access to data based on user role.
- C. Preventing certain types of devices from accessing data.
- D. Preventing data from being placed in unprotected storage.

**Answer:** B

#### NEW QUESTION 46

Organizations understand there are aggregation risks associated with the way the process their customer's data. They typically include the details of this aggregation risk in a privacy notice and ask that all customers acknowledge they understand these risks and consent to the processing. What type of risk response does this notice and consent represent?

- A. Risk transfer.
- B. Risk mitigation.
- C. Risk avoidance.
- D. Risk acceptance.

**Answer:** A

#### NEW QUESTION 48

Which of the following functionalities can meet some of the General Data Protection Regulation's (GDPR's) Data Portability requirements for a social networking app designed for users in the EU?

- A. Allow users to modify the data they provided the app.
- B. Allow users to delete the content they provided the app.
- C. Allow users to download the content they have provided the app.
- D. Allow users to get a time-stamped list of what they have provided the app.

**Answer:** C

#### NEW QUESTION 51

##### SCENARIO

Please use the following to answer next question:

EnsureClaim is developing a mobile app platform for managing data used for assessing car accident insurance claims. Individuals use the app to take pictures at the crash site, eliminating the need for a built-in vehicle camera. EnsureClaim uses a third-party hosting provider to store data collected by the app. EnsureClaim customer service employees also receive and review app data before sharing with insurance claim adjusters.

The app collects the following information: First and last name

Date of birth (DOB) Mailing address Email address

Car VIN number Car model License plate

Insurance card number Photo

Vehicle diagnostics Geolocation

The app is designed to collect and transmit geolocation data. How can data collection best be limited to the necessary minimum?

- A. Allow user to opt-out geolocation data collection at any time.
- B. Allow access and sharing of geolocation data only after an accident occurs.
- C. Present a clear and explicit Explanation about need for the geolocation data.
- D. Obtain consent and capture geolocation data at all times after consent is received.

**Answer:** D

#### NEW QUESTION 52

What would be an example of an organization transferring the risks associated with a data breach?

- A. Using a third-party service to process credit card transactions.
- B. Encrypting sensitive personal data during collection and storage
- C. Purchasing insurance to cover the organization in case of a breach.
- D. Applying industry standard data handling practices to the organization' practices.

Answer: C

### NEW QUESTION 57

#### SCENARIO

Carol was a U.S.-based glassmaker who sold her work at art festivals. She kept things simple by only accepting cash and personal checks.

As business grew, Carol couldn't keep up with demand, and traveling to festivals became burdensome. Carol opened a small boutique and hired Sam to run it while she worked in the studio. Sam was a natural salesperson, and business doubled. Carol told Sam, "I don't know what you are doing, but keep doing it!"

But months later, the gift shop was in chaos. Carol realized that Sam needed help so she hired Jane, who had business expertise and could handle the back-office tasks. Sam would continue to focus on sales. Carol gave Jane a few weeks to get acquainted with the artisan craft business, and then scheduled a meeting for the three of them to discuss Jane's first impressions.

At the meeting, Carol could not wait to hear Jane's thoughts, but she was unprepared for what Jane had to say. "Carol, I know that he doesn't realize it, but some of Sam's efforts to increase sales have put you in a vulnerable position. You are not protecting customers' personal information like you should."

Sam said, "I am protecting our information. I keep it in the safe with our bank deposit. It's only a list of customers' names, addresses and phone numbers that I get from their checks before I deposit them. I contact them when you finish a piece that I think they would like. That's the only information I have! The only other thing I do is post photos and information about your work on the photo sharing site that I use with family and friends. I provide my email address and people send me their information if they want to see more of your work. Posting online really helps sales, Carol. In fact, the only complaint I hear is about having to come into the shop to make a purchase."

Carol replied, "Jane, that doesn't sound so bad. Could you just fix things and help us to post even more online?"

"I can," said Jane. "But it's not quite that simple. I need to set up a new program to make sure that we follow the best practices in data management. And I am concerned for our customers. They should be able to manage how we use their personal information. We also should develop a social media strategy."

Sam and Jane worked hard during the following year. One of the decisions they made was to contract with an outside vendor to manage online sales. At the end of the year, Carol shared some exciting news. "Sam and Jane, you have done such a great job that one of the biggest names in the glass business wants to buy us out! And Jane, they want to talk to you about merging all of our customer and vendor information with theirs beforehand."

What type of principles would be the best guide for Jane's ideas regarding a new data management program?

- A. Collection limitation principles.
- B. Vendor management principles.
- C. Incident preparedness principles.
- D. Fair Information Practice Principles

Answer: D

### NEW QUESTION 61

In day to day interactions with technology, consumers are presented with privacy choices. Which of the following best represents the Privacy by Design (PbD) methodology of letting the user choose a non-zero-sum choice?

- A. Using images, words, and contexts to elicit positive feelings that result in proactive behavior, thus eliminating negativity and biases.
- B. Providing plain-language design choices that elicit privacy-related responses, helping users avoid errors and minimize the negative consequences of errors when they do occur.
- C. Displaying the percentage of users that chose a particular option, thus enabling the user to choose the most preferred option.
- D. Using contexts, antecedent events, and other priming concepts to assist the user in making a better privacy choice.

Answer: B

### NEW QUESTION 65

When analyzing user data, how is differential privacy applied?

- A. By injecting noise into aggregated datasets.
- B. By assessing differences between datasets.
- C. By applying asymmetric encryption to datasets.
- D. By removing personal identifiers from datasets.

Answer: A

### NEW QUESTION 70

#### SCENARIO

It should be the most secure location housing data in all of Europe, if not the world. The Global Finance Data Collective (GFDC) stores financial information and other types of client data from large banks, insurance companies, multinational corporations and governmental agencies. After a long climb on a mountain road that leads only to the facility, you arrive at the security booth. Your credentials are checked and checked again by the guard to visually verify that you are the person pictured on your passport and national identification card. You are led down a long corridor with server rooms on each side, secured by combination locks built into the doors. You climb a flight of stairs and are led into an office that is lighted brilliantly by skylights where the GFDC Director of Security, Dr. Monique Batch, greets you. On the far wall you notice a bank of video screens showing different rooms in the facility. At the far end, several screens show different sections of the road up the mountain

Dr. Batch explains once again your mission. As a data security auditor and consultant, it is a dream assignment: The GFDC does not want simply adequate controls, but the best and most effective security that current technologies allow.

"We were hacked twice last year," Dr. Batch says, "and although only a small number of records were stolen, the bad press impacted our business. Our clients count on us to provide security that is nothing short of impenetrable and to do so quietly. We hope to never make the news again." She notes that it is also essential that the facility is in compliance with all relevant security regulations and standards.

You have been asked to verify compliance as well as to evaluate all current security controls and security measures, including data encryption methods, authentication controls and the safest methods for transferring data into and out of the facility. As you prepare to begin your analysis, you find yourself considering an intriguing question: Can these people be sure that I am who I say I am?

You are shown to the office made available to you and are provided with system login information, including the name of the wireless network and a wireless key. Still pondering, you attempt to pull up the facility's wireless network, but no networks appear in the wireless list. When you search for the wireless network by name, however it is readily found.

Why would you recommend that GFC use record encryption rather than disk, file or table encryption?

- A. Record encryption is asymmetric, a stronger control measure.
- B. Record encryption is granular, limiting the damage of potential breaches.
- C. Record encryption involves tag masking, so its metadata cannot be decrypted

D. Record encryption allows for encryption of personal data only.

**Answer: B**

### NEW QUESTION 73

#### SCENARIO

Carol was a U.S.-based glassmaker who sold her work at art festivals. She kept things simple by only accepting cash and personal checks.

As business grew, Carol couldn't keep up with demand, and traveling to festivals became burdensome. Carol opened a small boutique and hired Sam to run it while she worked in the studio. Sam was a natural salesperson, and business doubled. Carol told Sam, "I don't know what you are doing, but keep doing it!"

But months later, the gift shop was in chaos. Carol realized that Sam needed help so she hired Jane, who had business expertise and could handle the back-office tasks. Sam would continue to focus on sales. Carol gave Jane a few weeks to get acquainted with the artisan craft business, and then scheduled a meeting for the three of them to discuss Jane's first impressions.

At the meeting, Carol could not wait to hear Jane's thoughts, but she was unprepared for what Jane had to say. "Carol, I know that he doesn't realize it, but some of Sam's efforts to increase sales have put you in a vulnerable position. You are not protecting customers' personal information like you should."

Sam said, "I am protecting our information. I keep it in the safe with our bank deposit. It's only a list of

customers' names, addresses and phone numbers that I get from their checks before I deposit them. I contact them when you finish a piece that I think they would like. That's the only information I have! The only other thing I do is post photos and information about your work on the photo sharing site that I use with family and friends. I provide my email address and people send me their information if they want to see more of your work. Posting online really helps sales, Carol. In fact, the only complaint I hear is about having to come into the shop to make a purchase."

Carol replied, "Jane, that doesn't sound so bad. Could you just fix things and help us to post even more online?"

"I can," said Jane. "But it's not quite that simple. I need to set up a new program to make sure that we follow the best practices in data management. And I am concerned for our customers. They should be able to manage how we use their personal information. We also should develop a social media strategy."

Sam and Jane worked hard during the following year. One of the decisions they made was to contract with an outside vendor to manage online sales. At the end of the year, Carol shared some exciting news. "Sam and Jane, you have done such a great job that one of the biggest names in the glass business wants to buy us out! And Jane, they want to talk to you about merging all of our customer and vendor information with theirs beforehand."

Which regulator has jurisdiction over the shop's data management practices?

- A. The Federal Trade Commission.
- B. The Department of Commerce.
- C. The Data Protection Authority.
- D. The Federal Communications Commission.

**Answer: A**

### NEW QUESTION 78

You are a wine collector who uses the web to do research about your hobby. You navigate to a news site and an ad for wine pops up. What kind of advertising is this?

- A. Remnant.
- B. Behavioral.
- C. Contextual.
- D. Demographic.

**Answer: B**

### NEW QUESTION 82

Which of the following is the least effective privacy preserving practice in the Systems Development Life Cycle (SDLC)?

- A. Conducting privacy threat modeling for the use-case.
- B. Following secure and privacy coding standards in the development.
- C. Developing data flow modeling to identify sources and destinations of sensitive data.
- D. Reviewing the code against Open Web Application Security Project (OWASP) Top 10 Security Risks.

**Answer: C**

### NEW QUESTION 86

Which of the following became a foundation for privacy principles and practices of countries and organizations across the globe?

- A. The Personal Data Ordinance.
- B. The EU Data Protection Directive.
- C. The Code of Fair Information Practices.
- D. The Organization for Economic Co-operation and Development (OECD) Privacy Principles.

**Answer: D**

### NEW QUESTION 89

#### SCENARIO

Please use the following to answer the next question:

Chuck, a compliance auditor for a consulting firm focusing on healthcare clients, was required to travel to the client's office to perform an onsite review of the client's operations. He rented a car from Finley Motors upon arrival at the airport as so he could commute to and from the client's office. The car rental agreement was electronically signed by Chuck and included his name, address, driver's license, make/model of the car, billing rate, and additional details describing the rental transaction. On the second night, Chuck was caught by a red light camera not stopping at an intersection on his way to dinner. Chuck returned the car back to the car rental agency at the end week without mentioning the infraction and Finley Motors emailed a copy of the final receipt to the address on file.

Local law enforcement later reviewed the red light camera footage. As Finley Motors is the registered owner of the car, a notice was sent to them indicating the infraction and fine incurred. This notice included the license plate number, occurrence date and time, a photograph of the driver, and a web portal link to a video clip of the violation for further review. Finley Motors, however, was not responsible for the violation as they were not driving the car at the time and transferred the incident to AMP Payment Resources for further review. AMP Payment Resources identified Chuck as the driver based on the rental agreement he signed when picking up the car and then contacted Chuck directly through a written letter regarding the infraction to collect the fine.

After reviewing the incident through the AMP Payment Resources' web portal, Chuck paid the fine using his personal credit card. Two weeks later, Finley Motors sent Chuck an email promotion offering 10% off a future rental.

What is the most secure method Finley Motors should use to transmit Chuck's information to AMP Payment Resources?

- A. Cloud file transfer services.
- B. Certificate Authority (CA).
- C. HyperText Transfer Protocol (HTTP).
- D. Transport Layer Security (TLS).

**Answer: D**

#### NEW QUESTION 90

Which is NOT a suitable action to apply to data when the retention period ends?

- A. Aggregation.
- B. De-identification.
- C. Deletion.
- D. Retagging.

**Answer: C**

#### NEW QUESTION 93

What is a mistake organizations make when establishing privacy settings during the development of applications?

- A. Providing a user with too many choices.
- B. Failing to use "Do Not Track" technology.
- C. Providing a user with too much third-party information.
- D. Failing to get explicit consent from a user on the use of cookies.

**Answer: D**

#### NEW QUESTION 95

What logs should an application server retain in order to prevent phishing attacks while minimizing data retention?

- A. Limited-retention, de-identified logs including only metadata.
- B. Limited-retention, de-identified logs including the links clicked in messages as well as metadata.
- C. Limited-retention logs including the identity of parties sending and receiving messages as well as metadata.
- D. Limited-retention logs including the links clicked in messages, the identity of parties sending and receiving them, as well as metadata.

**Answer: B**

#### NEW QUESTION 96

Which of the following would be the best method of ensuring that Information Technology projects follow Privacy by Design (PbD) principles?

- A. Develop a technical privacy framework that integrates with the development lifecycle.
- B. Utilize Privacy Enhancing Technologies (PETs) as a part of product risk assessment and management.
- C. Identify the privacy requirements as a part of the Privacy Impact Assessment (PIA) process during development and evaluation stages.
- D. Develop training programs that aid the developers in understanding how to turn privacy requirements into actionable code and design level specifications.

**Answer: D**

#### NEW QUESTION 97

Aadhaar is a unique-identity number of 12 digits issued to all Indian residents based on their biometric and demographic data. The data is collected by the Unique Identification Authority of India. The Aadhaar database contains the Aadhaar number, name, date of birth, gender and address of over 1 billion individuals.

Which of the following datasets derived from that data would be considered the most de-identified?

- A. A count of the years of birth and hash of the person's gender.
- B. A count of the month of birth and hash of the person's first name.
- C. A count of the day of birth and hash of the person's first initial of their first name.
- D. Account of the century of birth and hash of the last 3 digits of the person's Aadhaar number.

**Answer: C**

#### NEW QUESTION 99

##### SCENARIO

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving. However, the company now sells online through retail sites designated for industries and demographics, sites such as "My Cool Ride" for automobile-related products or "Zoomer" for gear aimed toward young adults. The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.

You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company's culture. For this project, you are considering using a series of third-party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company's product lines as well as products from affiliates. This new omnibus site will be known, aptly, as "Under the Sun." The Director of Marketing wants the site not only to sell Ancillary's products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

If you are asked to advise on privacy concerns regarding paid advertisements, which is the most important aspect to cover?

- A. Unseen web beacons that combine information on multiple users.
- B. Latent keys that trigger malware when an advertisement is selected.
- C. Personal information collected by cookies linked to the advertising network.
- D. Sensitive information from Structured Query Language (SQL) commands that may be exposed.

**Answer: C**

#### NEW QUESTION 101

Which of the following is an example of the privacy risks associated with the Internet of Things (IoT)?

- A. A group of hackers infiltrate a power grid and cause a major blackout.
- B. An insurance company raises a person's rates based on driving habits gathered from a connected car.
- C. A website stores a cookie on a user's hard drive so the website can recognize the user on subsequent visits.
- D. A water district fines an individual after a meter reading reveals excess water use during drought conditions.

**Answer: B**

#### NEW QUESTION 105

##### SCENARIO

Please use the following to answer next question:

EnsureClaim is developing a mobile app platform for managing data used for assessing car accident insurance claims. Individuals use the app to take pictures at the crash site, eliminating the need for a built-in vehicle camera. EnsureClaim uses a third-party hosting provider to store data collected by the app. EnsureClaim customer service employees also receive and review app data before sharing with insurance claim adjusters.

The app collects the following information: First and last name

Date of birth (DOB) Mailing address Email address

Car VIN number Car model License plate

Insurance card number Photo

Vehicle diagnostics

Geolocation

All of the following technical measures can be implemented by EnsureClaim to protect personal information that is accessible by third-parties EXCEPT?

- A. Encryption.
- B. Access Controls.
- C. De-identification.
- D. Multi-factor authentication.

**Answer: B**

#### NEW QUESTION 107

A company configures their information system to have the following capabilities: Allow for selective disclosure of attributes to certain parties, but not to others.

Permit the sharing of attribute references instead of attribute values - such as "I am over 21" instead of birthday date.

Allow for information to be altered or deleted as needed.

These capabilities help to achieve which privacy engineering objective?

- A. Predictability.
- B. Manageability.
- C. Disassociability.
- D. Integrity.

**Answer: C**

#### NEW QUESTION 112

Which of the following does NOT illustrate the 'respect to user privacy' principle?

- A. Implementing privacy elements within the user interface that facilitate the use of technology by any visually-challenged users.
- B. Enabling Data Subject Access Request (DSARs) that provide rights for correction, deletion, amendment and rectification of personal information.
- C. Developing a consent management self-service portal that enables the data subjects to review the details of consent provided to an organization.
- D. Filing breach notification paperwork with data protection authorities which detail the impact to data subjects.

**Answer: D**

#### NEW QUESTION 117

.....

## Relate Links

**100% Pass Your CIPT Exam with Exambible Prep Materials**

<https://www.exambible.com/CIPT-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>