

IAPP

Exam Questions CIPT

Certified Information Privacy Technologist



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

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 3

Which of the following would best improve an organization's system of limiting data use?

- A. Implementing digital rights management technology.
- B. Confirming implied consent for any secondary use of data.
- C. Applying audit trails to resources to monitor company personnel.
- D. Instituting a system of user authentication for company personnel.

Answer: C

NEW QUESTION 4

Between November 30th and December 2nd, 2013, cybercriminals successfully infected the credit card payment systems and bypassed security controls of a United States-based retailer with malware that exfiltrated 40 million credit card numbers. Six months prior, the retailer had malware detection software installed to prevent against such an attack.

Which of the following would best explain why the retailer's consumer data was still exfiltrated?

- A. The detection software alerted the retailer's security operations center per protocol, but the information security personnel failed to act upon the alerts.
- B. The U.S Department of Justice informed the retailer of the security breach on December 12th, but the retailer took three days to confirm the breach and eradicate the malware.
- C. The IT systems and security measures utilized by the retailer's third-party vendors were in compliance with industry standards, but their credentials were stolen by black hat hackers who then entered the retailer's system.
- D. The retailer's network that transferred personal data and customer payments was separate from the rest of the corporate network, but the malware code was disguised with the name of software that is supposed to protect this information.

Answer: B

NEW QUESTION 5

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 6

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 the 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 7

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.

Considering that LeadOps will host/process personal information on behalf of Clean-Q remotely, what is an appropriate next step for Clean-Q senior management to assess LeadOps' appropriateness?

- A. Nothing at this stage as the Managing Director has made a decision.
- B. Determine if any Clean-Q competitors currently use LeadOps as a solution.
- C. Obtain a legal opinion from an external law firm on contracts management.
- D. Involve the Information Security team to understand in more detail the types of services and solutions LeadOps is proposing.

Answer: D

NEW QUESTION 8

Which activity would best support the principle of data quality?

- A. Providing notice to the data subject regarding any change in the purpose for collecting such data.
- B. Ensuring that the number of teams processing personal information is limited.
- C. Delivering information in a format that the data subject understands.
- D. Ensuring that information remains accurate.

Answer: D

NEW QUESTION 9

A privacy engineer reviews a newly developed on-line registration page on a company's website. The purpose of the page is to enable corporate customers to submit a returns / refund request for physical goods. The page displays the following data capture fields: company name, account reference, company address, contact name, email address, contact phone number, product name, quantity, issue description and company bank account details. After her review, the privacy engineer recommends setting certain capture fields as "non-mandatory". Setting which of the following fields as "non-mandatory" would be the best example of the principle of data minimization?

- A. The contact phone number field.
- B. The company address and name.
- C. The contact name and email address.
- D. The company bank account detail field.

Answer: B

NEW QUESTION 10**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.

How can Finley Motors reduce the risk associated with transferring Chuck's personal information to AMP Payment Resources?

- A. By providing only the minimum necessary data to process the violation notice and masking all other information prior to transfer.
- B. By requesting AMP Payment Resources delete unnecessary datasets and only utilize what is necessary to process the violation notice.
- C. By obfuscating the minimum necessary data to process the violation notice and require AMP Payment Resources to secure store the personal information.
- D. By transferring all information to separate datafiles and requiring AMP Payment Resources to combine the datasets during processing of the violation notice.

Answer: A

NEW QUESTION 10**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 regulation most likely applies to the data stored by Berry Country Regional Medical Center?

- A. Personal Information Protection and Electronic Documents Act
- B. Health Insurance Portability and Accountability Act
- C. The Health Records Act 2001
- D. The European Union Directive 95/46/EC

Answer: A

NEW QUESTION 15

A valid argument against data minimization is that it?

- A. Can limit business opportunities.
- B. Decreases the speed of data transfers.
- C. Can have an adverse effect on data quality.
- D. Increases the chance that someone can be identified from data.

Answer: A

NEW QUESTION 19

A credit card with the last few numbers visible is an example of what?

- A. Masking data
- B. Synthetic data
- C. Sighting controls.
- D. Partial encryption

Answer: A

NEW QUESTION 22

An organization based in California, USA is implementing a new online helpdesk solution for recording customer call information. The organization considers the capture of personal data on the online helpdesk solution to be in the interest of the company in best servicing customer calls. Before implementation, a privacy technologist should conduct which of the following?

- A. A Data Protection Impact Assessment (DPIA) and consultation with the appropriate regulator to ensure legal compliance.
- B. A privacy risk and impact assessment to evaluate potential risks from the proposed processing operations.
- C. A Legitimate Interest Assessment (LIA) to ensure that the processing is proportionate and does not override the privacy, rights and freedoms of the customers.
- D. A security assessment of the help desk solution and provider to assess if the technology was developed with a security by design approach.

Answer: C

NEW QUESTION 25

Which of the following is a vulnerability of a sensitive biometrics authentication system?

- A. False positives.
- B. False negatives.
- C. Slow recognition speeds.
- D. Theft of finely individualized personal data.

Answer: C

NEW QUESTION 28

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 33

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 34

What is an Access Control List?

- A. A list of steps necessary for an individual to access a resource.
- B. A list that indicates the type of permission granted to each individual.
- C. A list showing the resources that an individual has permission to access.
- D. A list of individuals who have had their access privileges to a resource revoked.

Answer: C

NEW QUESTION 37

What is the main reason the Do Not Track (DNT) header is not acknowledged by more companies?

- A. Most web browsers incorporate the DNT feature.
- B. The financial penalties for violating DNT guidelines are too high.
- C. There is a lack of consensus about what the DNT header should mean.
- D. It has been difficult to solve the technological challenges surrounding DNT.

Answer: C

NEW QUESTION 42

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 45

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 50

Which Organization for Economic Co-operation and Development (OECD) privacy protection principle encourages an organization to obtain an individual’s consent before transferring personal information?

- A. Individual participation.
- B. Purpose specification.
- C. Collection limitation.
- D. Accountability.

Answer: C

NEW QUESTION 54

SCENARIO

Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company’s information security policy and industry standards. Kyle is also new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle’s schedule included participating in meetings and observing work in the IT and compliance departments.

Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization’s wireless network. Kyle would need to get up to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.

Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company’s privacy risk assessment, noting that the secondary use of personal information was considered a high risk.

By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn’t wait to recommend his friend Ben who would be perfect for the job.

Which data practice is Barney most likely focused on improving?

- A. Deletion
- B. Inventory.
- C. Retention.
- D. Sharing

Answer: C

NEW QUESTION 55

What is the best way to protect privacy on a geographic information system (GIS)?

- A. Limiting the data provided to the system.
- B. Using a wireless encryption protocol.
- C. Scrambling location information.
- D. Using a firewall.

Answer: A

NEW QUESTION 58

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.

What type of wireless network does GFDC seem to employ?

- A. A hidden network.
- B. A reluctant network.
- C. A user verified network.
- D. A wireless mesh network.

Answer: A

NEW QUESTION 63

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 64

Which of the following CANNOT be effectively determined during a code audit?

- A. Whether access control logic is recommended in all cases.
- B. Whether data is being incorrectly shared with a third-party.
- C. Whether consent is durably recorded in the case of a server crash.
- D. Whether the differential privacy implementation correctly anonymizes data.

Answer: D

NEW QUESTION 65

What is the term for information provided to a social network by a member?

- A. Profile data.
- B. Declared data.
- C. Personal choice data.
- D. Identifier information.

Answer: A

NEW QUESTION 69

A user who owns a resource wants to give other individuals access to the resource. What control would apply?

- A. Mandatory access control.
- B. Role-based access controls.
- C. Discretionary access control.
- D. Context of authority controls.

Answer: B

NEW QUESTION 74

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, Clear-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 on a 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.

What is a key consideration for assessing external service providers like LeadOps, which will conduct personal information processing operations on Clean-Q's behalf?

- A. Understanding LeadOps' costing model.
- B. Establishing a relationship with the Managing Director of LeadOps.
- C. Recognizing the value of LeadOps' website holding a verified security certificate.
- D. Obtaining knowledge of LeadOps' information handling practices and information security environment.

Answer: D

NEW QUESTION 76

Which of the following statements describes an acceptable disclosure practice?

- A. An organization's privacy policy discloses how data will be used among groups within the organization itself.
- B. With regard to limitation of use, internal disclosure policies override contractual agreements with third parties.
- C. Intermediaries processing sensitive data on behalf of an organization require stricter disclosure oversight than vendors.
- D. When an organization discloses data to a vendor, the terms of the vendor's privacy notice prevail over the organization's privacy notice.

Answer: A

NEW QUESTION 79

What is the most important requirement to fulfill when transferring data out of an organization?

- A. Ensuring the organization sending the data controls how the data is tagged by the receiver.
- B. Ensuring the organization receiving the data performs a privacy impact assessment.
- C. Ensuring the commitments made to the data owner are followed.
- D. Extending the data retention schedule as needed.

Answer: C

NEW QUESTION 83

SCENARIO

Wesley Energy has finally made its move, acquiring the venerable oil and gas exploration firm Lancelot from its long-time owner David Wilson. As a member of the transition team, you have come to realize that Wilson's quirky nature affected even Lancelot's data practices, which are maddeningly inconsistent. "The old man hired and fired IT people like he was changing his necktie," one of Wilson's seasoned lieutenants tells you, as you identify the traces of initiatives left half complete.

For instance, while some proprietary data and personal information on clients and employees is encrypted, other sensitive information, including health information from surveillance testing of employees for toxic exposures, remains unencrypted, particularly when included within longer records with less-sensitive data. You also find that data is scattered across applications, servers and facilities in a manner that at first glance seems almost random.

Among your preliminary findings of the condition of data at Lancelot are the following:

- Cloud technology is supplied by vendors around the world, including firms that you have not heard of.
- You are told by a former Lancelot employee that these vendors operate with divergent security requirements and protocols.
- The company's proprietary recovery process for shale oil is stored on servers among a variety of less-sensitive information that can be accessed not only by scientists, but by personnel of all types at most company locations.
 - DES is the strongest encryption algorithm currently used for any file.
 - Several company facilities lack physical security controls, beyond visitor check-in, which familiar vendors often bypass.
 - Fixing all of this will take work, but first you need to grasp the scope of the mess and formulate a plan of action to address it.

Which procedure should be employed to identify the types and locations of data held by Wesley Energy?

- A. Privacy audit.
- B. Log collection
- C. Data inventory.
- D. Data classification.

Answer: C

NEW QUESTION 86

After committing to a Privacy by Design program, which activity should take place first?

- A. Create a privacy standard that applies to all projects and services.
- B. Establish a retention policy for all data being collected.
- C. Implement easy to use privacy settings for users.
- D. Perform privacy reviews on new projects.

Answer: B

NEW QUESTION 88**SCENARIO**

Tom looked forward to starting his new position with a U.S —based automobile leasing company (New Company), now operating in 32 states. New Company was recently formed through the merger of two prominent players, one from the eastern region (East Company) and one from the western region (West Company). Tom, a Certified Information Privacy Technologist (CIPT), is New Company's first Information Privacy and Security Officer. He met today with Dick from East Company, and Harry, from West Company. Dick and Harry are veteran senior information privacy and security professionals at their respective companies, and continue to lead the east and west divisions of New Company. The purpose of the meeting was to conduct a SWOT (strengths/weaknesses/opportunities/threats) analysis for New Company. Their SWOT analysis conclusions are summarized below.

Dick was enthusiastic about an opportunity for the New Company to reduce costs and increase computing power and flexibility through cloud services. East Company had been contemplating moving to the cloud, but West Company already had a vendor that was providing it with software-as-a-service (SaaS). Dick was looking forward to extending this service to the eastern region. Harry noted that this was a threat as well, because West Company had to rely on the third party to protect its data.

Tom mentioned that neither of the legacy companies had sufficient data storage space to meet the projected growth of New Company, which he saw as a weakness. Tom stated that one of the team's first projects would be to construct a consolidated New Company data warehouse. Tom would personally lead this project and would be held accountable if information was modified during transmission to or during storage in the new data warehouse.

Tom, Dick and Harry agreed that employee network access could be considered both a strength and a weakness. East Company and West Company had strong performance records in this regard; both had robust network access controls that were working as designed. However, during a projected year-long transition period, New Company employees would need to be able to connect to a New Company network while retaining access to the East Company and West Company networks.

Which statement is correct about addressing New Company stakeholders' expectations for privacy?

- A. New Company should expect consumers to read the company's privacy policy.
- B. New Company should manage stakeholder expectations for privacy even when the stakeholders' data is not held by New Company.
- C. New Company would best meet consumer expectations for privacy by adhering to legal requirements.
- D. New Company's commitment to stakeholders ends when the stakeholders' data leaves New Company.

Answer: D

NEW QUESTION 89**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 94

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 96**SCENARIO**

Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company's information security policy and industry standards. Kyle is also new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle's schedule included participating in meetings and observing work in the IT and compliance departments.

Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization's wireless network. Kyle would need to get up to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.

Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company's privacy risk assessment, noting that the secondary use of personal information was considered a high risk.

By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn't wait to recommend his friend Ben who would be perfect for the job.

Ted's implementation is most likely a response to what incident?

- A. Encryption keys were previously unavailable to the organization's cloud storage host.
- B. Signatureless advanced malware was detected at multiple points on the organization's networks.
- C. Cyber criminals accessed proprietary data by running automated authentication attacks on the organization's network.
- D. Confidential information discussed during a strategic teleconference was intercepted by the organization's top competitor.

Answer: A

NEW QUESTION 97

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CIPT Practice Exam Features:

- * CIPT Questions and Answers Updated Frequently
- * CIPT Practice Questions Verified by Expert Senior Certified Staff
- * CIPT Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CIPT Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CIPT Practice Test Here](#)