IAPP

Exam Questions CIPT

Certified Information Privacy Technologist

NEW QUESTION 1
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 2
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
What IT architecture would be most appropriate for this mobile platform?

A. Peer-to-peer architecture.
B. Client-server architecture.
C. Plug-in-based architecture.
D. Service-oriented architecture.

Answer: D

NEW QUESTION 3
What is the main function of the Amnesic Incognito Live System or TAILS device?

A. It allows the user to run a self-contained computer from a USB device.
B. It accesses systems with a credential that leaves no discernable tracks.
C. It encrypts data stored on any computer on a network.
D. It causes a system to suspend its security protocols.

Answer: A

NEW QUESTION 4
When should code audits be concluded?

A. At code check-in time.
B. At engineering design time.
C. While code is being sent to production.
D. Before launch after all code for a feature is complete.

Answer: D

NEW QUESTION 5
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 De
C. 12th, but the retailer took three days to confirm the breach and eradicate the malware.
D. 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.
E. 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 6
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 7
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 8
What term describes two re-identifiable data sets that both come from the same unidentified individual?

A. Pseudonymous data.
B. Anonymous data.
C. Aggregated data.
D. Imprecise data.

Answer: B

NEW QUESTION 9
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
Which of the following is considered a records management best practice?

A. Archiving expired data records and files.
B. Storing decryption keys with their associated backup systems.
C. Implementing consistent handling practices across all record types.
D. Using classification to determine access rules and retention policy.

Answer: D

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 13
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 18
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 21
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 23
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
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 31
A key principle of an effective privacy policy is that it should be?

A. Written in enough detail to cover the majority of likely scenarios.
B. Made general enough to maximize flexibility in its application.
C. Presented with external parties as the intended audience.
D. Designed primarily by the organization's lawyers.

Answer: C

NEW QUESTION 35
Which of the following are the mandatory pieces of information to be included in the documentation of records of processing activities for an organization that processes personal data on behalf of another organization?

A. Copies of the consent forms from each data subject.
B. Time limits for erasure of different categories of data.
C. Contact details of the processor and Data Protection Offer (DPO).
D. Descriptions of the processing activities and relevant data subjects.

Answer: B

NEW QUESTION 37
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 42
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 43
What distinguishes a "smart" device?

A. It can perform multiple data functions simultaneously.
B. It is programmable by a user without specialized training.
C. It can reapply access controls stored in its internal memory.
D. It augments its intelligence with information from the internet.

Answer: D

NEW QUESTION 47
Which technique is most likely to facilitate the deletion of every instance of data associated with a deleted user account from every data store held by an organization?

A. Auditing the code which deletes user accounts.
B. Building a standardized and documented retention program for user data deletion.
C. Monitoring each data store for presence of data associated with the deleted user account.
D. Training engineering teams on the importance of deleting user accounts their associated data from all data stores when requested.

Answer: C

NEW QUESTION 48
Which is NOT a way to validate a person's identity?

A. Swiping a smartcard into an electronic reader.
B. Using a program that creates random passwords.
C. Answering a question about "something you know".
D. Selecting a picture and tracing a unique pattern on it

Answer: B

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
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 measures can protect client information stored at GFDC?

A. De-linking of data into client-specific packets.
B. Cloud-based applications.
C. Server-side controls.
D. Data pruning

Answer: A

NEW QUESTION 54
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.
The Privacy Team is conducting a Privacy Impact Assessment (PIA) for the new Light Blue Health application currently in development. Which of the following best describes a risk that is likely to result in a privacy breach?

A. Limiting access to the app to authorized personnel.
B. Including non-transparent policies, terms and conditions in the app.
C. Insufficiently deleting personal data after an account reaches its retention period.
D. Not encrypting the health record when it is transferred to the Light Blue Health servers.

Answer: A

NEW QUESTION 57
How does k-anonymity help to protect privacy in micro data sets?

A. By ensuring that every record in a set is part of a group of "k" records having similar identifying information.
B. By switching values between records in order to preserve most statistics while still maintaining privacy.
C. By adding sufficient noise to the data in order to hide the impact of any one individual.
D. By top-coding all age data above a value of "k."

Answer: A

NEW QUESTION 59
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 63
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 68
A company seeking to hire engineers in Silicon Valley ran an ad campaign targeting women in a specific age range who live in the San Francisco Bay Area. Which Calo objective privacy harm is likely to result from this campaign?

A. Lost opportunity.
B. Economic loss.
C. Loss of liberty.
D. Social detriment.

Answer: D

NEW QUESTION 71
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 73
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 should Finley Motors have done to incorporate the transparency principle of Privacy by Design (PbD)?

A. Signed a data sharing agreement with AMP Payment Resources.
B. Documented that Finley Motors has a legitimate interest to share Chuck's information.
C. Obtained verbal consent from Chuck and recorded it within internal systems.
D. Provided notice of data sharing practices within the electronically signed rental agreement.

Answer: D

NEW QUESTION 77
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 79
A privacy engineer has been asked to review an online account login page. He finds there is no limitation on the number of invalid login attempts a user can make when logging into their online account.
What would be the best recommendation to minimize the potential privacy risk from this weakness?

A. Implement a CAPTCHA system.
B. Develop server-side input validation checks.
C. Enforce strong password and account credentials.
D. Implement strong Transport Layer Security (TLS) to ensure an encrypted link.

Answer: B

NEW QUESTION 83
After downloading and loading a mobile app, the user is presented with an account registration page requesting the user to provide certain personal details. Two statements are also displayed on the same page along with a box for the user to check to indicate their confirmation:
Statement 1 reads: “Please check this box to confirm you have read and accept the terms and conditions of the end user license agreement” and includes a hyperlink to the terms and conditions.
Statement 2 reads: “Please check this box to confirm you have read and understood the privacy notice” and includes a hyperlink to the privacy notice.
Under the General Data Protection Regulation (GDPR), what lawful basis would you primarily except the privacy notice to refer to?

A. Consent.
B. Vital interests.
C. Legal obligation.
D. Legitimate interests.

Answer: A

NEW QUESTION 87
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 90
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.
Why is Jordan’s claim that the company does not collect personal information as identified by the GDPR inaccurate?

A. The potential customers must browse for products online.
B. The fitness trackers capture sleep and heart rate data to monitor an individual’s behavior.
C. The website collects the customers’ and users’ region and country information.
D. The customers must pair their fitness trackers to either smartphones or computers.

Answer: A

NEW QUESTION 95
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.
What technology is under consideration in the first project in this scenario?

A. Server driven controls.
B. Cloud computing
C. Data on demand
D. MAC filtering

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 - Questons 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