CIPT

CIPT

Website: https://vceplus.com
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

https://vceplus.com/

Exam A

QUESTION 1
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://privacyrights.org/resources/review-fair-information-principles-foundation-privacy-public-policy

QUESTION 3
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 of the following should Kyle recommend to Jill as the best source of support for her initiative?

A. Investors.
B. Regulators.
C. Industry groups.
D. Corporate researchers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://iapp.org/resources/article/fair-information-practices/

QUESTION 7
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.

Correct Answer: C

Explanation/Reference:
Reference: http://oecdprivacy.org

QUESTION 8
Granting data subjects the right to have data corrected, amended, or deleted describes?

A. Use limitation.
B. Accountability.
C. A security safeguard
D. Individual participation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ncbi.nlm.nih.gov/books/NBK236546/

QUESTION 9
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following suggests the greatest degree of transparency?

A. A privacy disclosure statement clearly articulates general purposes for collection
B. The data subject has multiple opportunities to opt-out after collection has occurred.
C. A privacy notice accommodates broadly defined future collections for new products.
D. After reading the privacy notice, a data subject confidently infers how her information will be used.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
What is the **main** reason a company relies on implied consent instead of explicit consent from a user to process her data?

A. The implied consent model provides the user with more detailed data collection information.
B. To secure explicit consent, a user's website browsing would be significantly disrupted.
C. An explicit consent model is more expensive to implement.
D. Regulators prefer the implied consent model.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
What is the **main** benefit of using dummy data during software testing?

A. The data comes in a format convenient for testing.
B. Statistical disclosure controls are applied to the data.
C. The data enables the suppression of particular values in a set.
D. Developers do not need special privacy training to test the software.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://cloud.google.com/storage/docs/gsutil/addlhelp/WorkingWithObjectMetadata

QUESTION 14
What must be done to destroy data stored on "write once read many" (WORM) media?

A. The data must be made inaccessible by encryption.
B. The erase function must be used to remove all data.
C. The media must be physically destroyed.
D. The media must be reformatted.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

Which of the following provides a mechanism that allows an end-user to use a single sign-on (SSO) for multiple services?

A. The Open ID Federation.
B. PCI Data Security Standards Council
C. International Organization for Standardization.
D. Personal Information Protection and Electronic Documents Act.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 16
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/bs-latn-ba/azure/role-based-access-control/overview

QUESTION 17
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.

makes data impenetrable to attacks.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sciencedirect.com/topics/computer-science/homomorphic-encryption

QUESTION 18
What has been found to undermine the public key infrastructure system?

A. Man-in-the-middle attacks.
B. Inability to track abandoned keys.
C. Disreputable certificate authorities.
D. Browsers missing a copy of the certificate authority's public key.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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 is true regarding the type of encryption Lancelot uses?

A. It employs the data scrambling technique known as obfuscation.
B. Its decryption key is derived from its encryption key.
C. It uses a single key for encryption and decryption.
D. It is a data masking methodology.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://money.stackexchange.com/questions/98951/credit-card-number-masking-good-practices-rules-law-regulations

QUESTION 21
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 24
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.wired.co.uk/article/tails-operating-software

QUESTION 25
What is a **main** benefit of data aggregation?

A. It is a good way to perform analysis without needing a statistician.
B. It applies two or more layers of protection to a single data record.
C. It allows one to draw valid conclusions from small data samples.
D. It is a good way to achieve de-identification and unlinkabilty.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
When releasing aggregates, what must be performed to magnitude data to ensure privacy?

A. Value swapping.
B. Noise addition.
C. Basic rounding.
D. Top coding.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Reference: https://academic.oup.com/idpl/article/8/1/29/4930711

QUESTION 28
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://ico.org.uk/media/1061/anonymisation-code.pdf

QUESTION 29
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://inspiredelearning.com/blog/phishing-vs-pharming-whats-difference/

QUESTION 31
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://neilpatel.com/blog/behavioral-advertising/

QUESTION 32
Why is first-party web tracking very difficult to prevent?

A. The available tools to block tracking would break most sites' functionality.
B. Consumers enjoy the many benefits they receive from targeted advertising.
C. Regulatory frameworks are not concerned with web tracking.
D. Most browsers do not support automatic blocking.

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Reference: https://www.opentracker.net/article/third-party-cookies-vs-first-party-cookies

QUESTION 33
During a transport layer security (TLS) session, what happens immediately after the web browser creates a random PreMasterSecret?

A. The server decrypts the PremasterSecret.
B. The web browser opens a TLS connection to the PremasterSecret.
C. The web browser encrypts the PremasterSecret with the server's public key.
D. The server and client use the same algorithm to convert the PremasterSecret into an encryption key.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://books.google.com.pk/books?id=OaXise4B-p8C&pg=PA175&lpg=PA175&dq=iapp+During+a+transport+layer+security+(TLS)+session,+what +happens+immediately+after+the+web+browser+creates+a+random +PreMasterSecret&source=bl&ots=zR0RCfnx3c&sig=ACfU3U0bTOeOfPfcoq_Y95SZs6imKKilug&hl=en&sa=X&ved=2ahUKEwjkscDHpcbnAhUJuRoKHU5iC9cQ6 AEwCnoECAkQAQ#v=onepage&q=iapp%20During%20a%20transport%20layer%20security%20(TLS)%20session%2C%20what%20happens%20immediately% 20after%20the%20web%20browser%20creates%20a%20random%20PreMasterSecret&f=false

QUESTION 34
What is the **main** benefit of using a private cloud?

A. The ability to use a backup system for personal files.
B. The ability to outsource data support to a third party.
C. The ability to restrict data access to employees and contractors.
D. The ability to cut costs for storing, maintaining, and accessing data.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
In the realm of artificial intelligence, how has deep learning enabled greater implementation of machine learning?

A. By using hand-coded classifiers like edge detection filters so that a program can identify where an object starts and stops.
B. By increasing the size of neural networks and running massive amounts of data through the network to train it.
C. By using algorithmic approaches such as decision tree learning and inductive logic programming.
D. By hand coding software routines with a specific set of instructions to accomplish a task.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://towardsdatascience.com/notes-on-artificial-intelligence-ai-machine-learning-ml-and-deep-learning-dl-for-56e51a2071c2

QUESTION 38
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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.

Ina 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 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.

If Clean-Q were to utilize LeadOps' services, what is a contract clause that may be included in the agreement entered into with LeadOps?

A. A provision that holds LeadOps liable for a data breach involving Clean-Q's information.
B. A provision prescribing technical and organizational controls that LeadOps must implement.
C. A provision that requires LeadOps to notify Clean-Q of any suspected breaches of information that involves customer or resource information managed on behalf of Clean-Q.
D. A provision that allows Clean-Q to conduct audits of LeadOps' information processing and information security environment, at LeadOps' cost and at any time that Clean-Q requires.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
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.

Ina 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 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 41
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.

Ina 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 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?

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following is **NOT** a workplace surveillance best practice?

A. Check local privacy laws before putting surveillance in place.
B. Ensure surveillance is discreet so employees do not alter their behavior.
C. Once surveillance data has been gathered, limit exposure of the content.
D. Ensure the minimal amount of surveillance is performed to meet the objective.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A sensitive biometrics authentication system is particularly susceptible to?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://link.springer.com/article/10.1007/s41403-017-0026-8 **QUESTION 44**
What is true of providers of wireless technology?

A. They have the legal right in most countries to control and use any data on their systems.
B. They can see all unencrypted data that crosses the system.
C. They are typically exempt from data security regulations.
D. They routinely backup data that crosses their system.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
SCENARIO

WebTracker Limited is a cloud-based online marketing service located in London. Last year, WebTracker migrated its IT infrastructure to the cloud provider AmaZure, 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 AmaZure'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 AmaZure, 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 AmaZure 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 AmaZure and the appropriate institutions in the USA and the European Union.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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.

When employees are working remotely, they usually connect to a Wi-Fi network. What should Harry advise for maintaining company security in this situation?
A. Hiding wireless service set identifiers (SSID).
B. Retaining the password assigned by the network.
C. Employing Wired Equivalent Privacy (WEP) encryption.
D. Using tokens sent through HTTP sites to verify user identity.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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 data lifecycle phase needs the **most** attention at this Ontario medical center?

A. Retention
B. Disclosure
C. Collection
D. Use

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: