Certified Information Privacy Technologist

CIPT

iapp

CIPT
PRACTICE EXAM

An iapp publication

CIPT® Practice Exam

An IAPP Publication

v2.0

About the IAPP CIPT Practice Exam

The IAPP CIPT practice exam is designed to support your preparation for the CIPT certification exam. Developed using IAPP study resources as well as subject matter experts' practical knowledge of the topics set forth in the IAPP's CIPT body of knowledge (version 3.2.0), the practice exam can help identify your relative strengths and weaknesses in the major domains of the CIPT body of knowledge. It was developed to simulate the types and breadth of questions you may encounter on the CIPT certification exam and is intended for use as an aid to focus study.

A strong performance on the practice exam does not guarantee similar success on the certification exam.

All items on the IAPP CIPT practice exam were reviewed for accuracy at the time of publication.

The IAPP CIPT practice exam was developed independently of the CIPT certification exam and does not contain CIPT certification exam items in active use.

Do you have questions or comments?

Please contact us at training@iapp.org

The CIPT practice exam and rationales may not be reproduced in any manner other than for use by the original purchaser.

CIPP®, CIPP/A®, CIPP/C®, CIPP/E®, CIPP/G®, CIPP/US®, CIPM® and CIPT® are registered trademarks of the International Association of Privacy Professionals, Inc.

Table of Contents

Instructions

1. Print out the answer sheet that precedes the exam. Use this to indicate your selection for each question. If you prefer, you may use the highlighter feature of your PDF reader to indicate your response.

2. To simulate the certification exam, set a timer for 150 minutes (2.5 hours).

3. Complete the test without referring to the answer key or rationales.

4. Print out the answer key which follows the exam. Check your answers against the answer key.

5. For each correct response, place a "1" or a checkmark in the corresponding domain column of the answer key. Note, the domain is indicated by an unshaded box and corresponds to the domain listed in the body of knowledge. The letter in the box next to the unshaded box is the competency of the body of knowledge to which the question relates.

6. Add up the number of correct answers under each domain column.

7. To compare how you did in each domain, calculate your scores as a percent:
    a. Divide the number of correct answers by the total number of questions in that domain.
    b. Multiply that number by 100.

8. Consult the rationales for detailed explanations of each answer and the section of the body of knowledge to which the question relates.

Answer Sheet

1 Ⓐ Ⓑ Ⓒ Ⓓ	2 Ⓐ Ⓑ Ⓒ Ⓓ	3 Ⓐ Ⓑ Ⓒ Ⓓ	4 Ⓐ Ⓑ Ⓒ Ⓓ	5 Ⓐ Ⓑ Ⓒ Ⓓ
6 Ⓐ Ⓑ Ⓒ Ⓓ	7 Ⓐ Ⓑ Ⓒ Ⓓ	8 Ⓐ Ⓑ Ⓒ Ⓓ	9 Ⓐ Ⓑ Ⓒ Ⓓ	10 Ⓐ Ⓑ Ⓒ Ⓓ
11 Ⓐ Ⓑ Ⓒ Ⓓ	12 Ⓐ Ⓑ Ⓒ Ⓓ	13 Ⓐ Ⓑ Ⓒ Ⓓ	14 Ⓐ Ⓑ Ⓒ Ⓓ	15 Ⓐ Ⓑ Ⓒ Ⓓ
16 Ⓐ Ⓑ Ⓒ Ⓓ	17 Ⓐ Ⓑ Ⓒ Ⓓ	18 Ⓐ Ⓑ Ⓒ Ⓓ	19 Ⓐ Ⓑ Ⓒ Ⓓ	20 Ⓐ Ⓑ Ⓒ Ⓓ
21 Ⓐ Ⓑ Ⓒ Ⓓ	22 Ⓐ Ⓑ Ⓒ Ⓓ	23 Ⓐ Ⓑ Ⓒ Ⓓ	24 Ⓐ Ⓑ Ⓒ Ⓓ	25 Ⓐ Ⓑ Ⓒ Ⓓ
26 Ⓐ Ⓑ Ⓒ Ⓓ	27 Ⓐ Ⓑ Ⓒ Ⓓ	28 Ⓐ Ⓑ Ⓒ Ⓓ	29 Ⓐ Ⓑ Ⓒ Ⓓ	30 Ⓐ Ⓑ Ⓒ Ⓓ
31 Ⓐ Ⓑ Ⓒ Ⓓ	32 Ⓐ Ⓑ Ⓒ Ⓓ	33 Ⓐ Ⓑ Ⓒ Ⓓ	34 Ⓐ Ⓑ Ⓒ Ⓓ	35 Ⓐ Ⓑ Ⓒ Ⓓ
36 Ⓐ Ⓑ Ⓒ Ⓓ	37 Ⓐ Ⓑ Ⓒ Ⓓ	38 Ⓐ Ⓑ Ⓒ Ⓓ	39 Ⓐ Ⓑ Ⓒ Ⓓ	40 Ⓐ Ⓑ Ⓒ Ⓓ
41 Ⓐ Ⓑ Ⓒ Ⓓ	42 Ⓐ Ⓑ Ⓒ Ⓓ	43 Ⓐ Ⓑ Ⓒ Ⓓ	44 Ⓐ Ⓑ Ⓒ Ⓓ	45 Ⓐ Ⓑ Ⓒ Ⓓ
46 Ⓐ Ⓑ Ⓒ Ⓓ	47 Ⓐ Ⓑ Ⓒ Ⓓ	48 Ⓐ Ⓑ Ⓒ Ⓓ	49 Ⓐ Ⓑ Ⓒ Ⓓ	50 Ⓐ Ⓑ Ⓒ Ⓓ
51 Ⓐ Ⓑ Ⓒ Ⓓ	52 Ⓐ Ⓑ Ⓒ Ⓓ	53 Ⓐ Ⓑ Ⓒ Ⓓ	54 Ⓐ Ⓑ Ⓒ Ⓓ	55 Ⓐ Ⓑ Ⓒ Ⓓ
56 Ⓐ Ⓑ Ⓒ Ⓓ	57 Ⓐ Ⓑ Ⓒ Ⓓ	58 Ⓐ Ⓑ Ⓒ Ⓓ	59 Ⓐ Ⓑ Ⓒ Ⓓ	60 Ⓐ Ⓑ Ⓒ Ⓓ
61 Ⓐ Ⓑ Ⓒ Ⓓ	62 Ⓐ Ⓑ Ⓒ Ⓓ	63 Ⓐ Ⓑ Ⓒ Ⓓ	64 Ⓐ Ⓑ Ⓒ Ⓓ	65 Ⓐ Ⓑ Ⓒ Ⓓ
66 Ⓐ Ⓑ Ⓒ Ⓓ	67 Ⓐ Ⓑ Ⓒ Ⓓ	68 Ⓐ Ⓑ Ⓒ Ⓓ	69 Ⓐ Ⓑ Ⓒ Ⓓ	70 Ⓐ Ⓑ Ⓒ Ⓓ
71 Ⓐ Ⓑ Ⓒ Ⓓ	72 Ⓐ Ⓑ Ⓒ Ⓓ	73 Ⓐ Ⓑ Ⓒ Ⓓ	74 Ⓐ Ⓑ Ⓒ Ⓓ	75 Ⓐ Ⓑ Ⓒ Ⓓ
76 Ⓐ Ⓑ Ⓒ Ⓓ	77 Ⓐ Ⓑ Ⓒ Ⓓ	78 Ⓐ Ⓑ Ⓒ Ⓓ	79 Ⓐ Ⓑ Ⓒ Ⓓ	80 Ⓐ Ⓑ Ⓒ Ⓓ
81 Ⓐ Ⓑ Ⓒ Ⓓ	82 Ⓐ Ⓑ Ⓒ Ⓓ	83 Ⓐ Ⓑ Ⓒ Ⓓ	84 Ⓐ Ⓑ Ⓒ Ⓓ	85 Ⓐ Ⓑ Ⓒ Ⓓ
86 Ⓐ Ⓑ Ⓒ Ⓓ	87 Ⓐ Ⓑ Ⓒ Ⓓ	88 Ⓐ Ⓑ Ⓒ Ⓓ	89 Ⓐ Ⓑ Ⓒ Ⓓ	90 Ⓐ Ⓑ Ⓒ Ⓓ

CIPT Practice Exam

1. In the context of a large retailer implementing Privacy-by-Design principles, which of the following strategies would best ensure that customer data is protected throughout its life cycle?

   A. Encrypting customer data when it is at rest.
   B. Updating privacy policies and training staff on privacy practices regularly.
   C. Embedding privacy controls into each stage of the data processing life cycle.
   D. Providing access to customer data to the marketing department exclusively.

2. Jenny completed a purchase on a website and was presented with a pop-up box on the final page that read, “Thank you for your purchase! We will email you in the future about related product and services. Please select an option below to opt-out.” The three buttons below the message read, “Do Not Opt-Out,” “Decline” and “Skip This Step.” Jenny selected the option to “Skip This Step,” believing it was the best choice to continue her browsing experience. This is an example of which of the following?

   A. Dark pattern.
   B. Clickstream pattern.
   C. Guided marketing model.
   D. Ad choice design approach.

3. A cloud service provider wants to advertise the benefits of its service by publishing information that shows how its users have interacted with the platform. It plans to publish only aggregated data to not identify its customers. What would be a best practice before publishing its aggregated data?

   A. The company should review its legal basis for keeping the sales information and determine whether the customers have provided consent.
   B. The company should maintain a log of its employees that accessed the database to ensure the underlying data has not been modified prior to aggregation.
   C. The company should ensure its procedures for responding to information requests by customers allow it to correct any errors in the published data.
   D. The company should evaluate whether publicly available or other sources of information are sufficient to reconstruct the aggregated database and identify individuals.

4. A utility company discovers that it is missing first names for some of its customers. It purchases householder data from a credit reference agency to obtain names and attempt to find a match in their customer database. The two companies will apply a logical rule that attributes the utility bills and assigns liability for such debts to the individual with the most active credit history at an address. What kind of privacy threat is **most likely** to occur based on this scenario?

   A. The data could become distorted.
   B. An individual’s identity could be appropriated.
   C. The data could be used to identify an individual.
   D. An individual could be placed under illegal surveillance.

5. An organization is using Scrum methodology to develop in-house solutions for customer support, which involves how personal data of its customers is processed. During each sprint, the team examines the implications the changes have on customer privacy and ensures the process remains compliant with their privacy program. When a change occurs in the system during development, there is a change management procedure that triggers an evaluation of whether the engineering, design, implementation or testing requirements needs to change within the development process. This example is a component of which of the below?

   A. Code audit process.
   B. Code review process.
   C. Software evolution process.
   D. Runtime behavior monitoring.

6. Beth's client is keen on ensuring that her team considers privacy and data protection issues at every phase of each product's life cycle. Which of the following enables the team to test various phases of the life cycle for potential risks?

   A. Binding corporate rules (BCR).
   B. Transfer impact assessment (TIA).
   C. Record of processing activity (RoPA).
   D. Data protection impact assessment (DPIA).

7. Which of the following is a part of a privacy risk assessment?

   A. Privacy training and awareness.
   B. Data inventory and data mapping.
   C. Ongoing operations and maintenance.
   D. Software development and unit testing.

8. Which of the following statements about aggregated data sets is **TRUE**?

   A. Combining multiple partial-identifiers can lead to individuals becoming identifiable.
   B. Removing names from the data set will prevent the individual from becoming identified.
   C. Generalizing the date of birth to age makes this data point unattributable to an individual.
   D. Disclosing the data set with no outlier data points will ensure individuals cannot be identified.

9. For a large retailer, which of the following actions best demonstrates adherence to privacy principles during the data retention phase of the data life cycle?

   A. Allowing customers to request deletion of their data at any time but keeping a copy exclusively for internal use.
   B. Storing all customer data indefinitely to ensure it is always available for future analysis and potential future uses.
   C. Backing up customer data to multiple secure locations regularly to prevent data loss and ensure future retrieval of data.
   D. Implementing a strict data retention policy that automatically deletes customer data after a specified period unless retention is legally required.

SCENARIO I

Please use the following scenario to answer the next TWO questions.

You work at a large multinational organization that operates a global online marketplace. The organization is headquartered in the U.S. but has operations in Ireland and Australia. Individuals in almost every country of the world can join the platform. Once a user is on the platform, they can sell items to other users around the world.

The platform facilitates the sending of items, but individuals making purchases don't know from which country their items will arrive. The platform allows individuals to post reviews about both the items they buy and the sellers of the goods. Individuals must register and create an account to sell items or make purchases.

Traditionally, users have been able to mask certain elements of their identity to other users when they create an account. This includes selecting a nickname rather than using their real names, masking their locations, and hiding their contact details (phone numbers, email addresses, etc.). The real data is provided to your company but is masked to other users. At the time information was collected, users were assured that their personal details would not be shared with other users.

In the past few days there has been a significant drop in users and revenues. A new competitor is luring away your company's users – and getting a significant number of new users who have never used a platform like this one in the past.

The head of product development thinks customers are leaving the platform and going to the competitor because the competitor does not permit users to be anonymous on the site. The head of product development has convinced the CEO that customers trust the competitor's platform and products sold on the platform because they can see that the other customers are "real people" and know exactly who they are. You think that users are likely leaving the platform because your company suffered a massive data breach several months ago, and users have just received notices about the incident.

Your CEO now wants to remove the ability for new users to mask their identities. The CEO also wants to unmask existing users' identities. You have been working hard to explain to the CEO why this is not feasible, and given the current post-breach climate, not an advisable step.

10. Which of the following statements is **NOT** correct with respect to the unmasking of user identities?

    A. Unmasking existing users' identities could violate the GDPR and other laws and regulations regarding notice.
    B. Unmasking existing users' identities could invite potential class action claims and affect your company's reputation.
    C. Unmasking existing users' identities would constitute an unfair and deceptive trade practice under the FTC Act, Section 5.
    D. Unmasking existing users' identities would cause your company to gain customers and be better able to compete with competitors.

11. Allowing users the ability to mask their identities on the platform aligns with which of the FTC's Five Fair Information Practice Principles?

    A. Notice principle.
    B. Choice principle.
    C. Security principle.
    D. Transparency principle.

END OF SCENARIO I QUESTIONS

12. A vulnerability in the customer relationship management (CRM) software is being exploited by malicious hackers. The CRM vendor indicated that a quick-fix to the software will not be available for a week. The patch management process will take another 3 days to complete after receiving the quick-fix. What compensating control should be put in place to protect the CRM system and customers' personal data in the meantime?

    A. Inform customers about the situation and the potential risk to their personal data.
    B. Monitor the CRM system and review the system logs for anomalies on a daily basis.
    C. Shut down the CRM system until the patch is installed and email customers about delays.
    D. Shorten the testing period for the patch management process to release the patch sooner.

13. A company is developing a web-based chatbot that will ask customers to input information about preferences and hobbies to direct them to relevant products and services. Which of the following is the first step software developers should take to ensure only the data needed is collected?

    A. Work with stakeholders to clearly define the project's goals and identify which data components are necessary for success.
    B. Create logs for interactions with the chatbot to confirm customers understand and appropriately respond to the chatbot's questions.
    C. Develop processes to transform collected data so that developers cannot see customer's personal data unless necessary to perform their jobs.
    D. Leverage Open Web Application Security Project (OWASP) resources to avoid common vulnerabilities and protect confidentiality of collected information.

14. Jack is a privacy engineer working in a bank. DevOps is enhancing the user interface of the bank's mobile application and contemplating the use of an open-source library module for facial recognition. DevOps approached Jack for his guidance. What is the first step that Jack must take?

    A. Conduct a risk/benefits analysis of the open-source software.
    B. Test the open-source software in the bank sandbox environment.
    C. Review and interpret the bank's policy on the use of open-source software.
    D. Contact the developer about the level of support for the open-source software.

15. When implementing privacy by design, the processing and use of personal data should not be obscured or obfuscated. Notice and disclosure regarding the use or personal data should consider the needs of the audience. Which of the following is a foundational privacy principle that **best** reflects this statement?

    A. Transparency.
    B. Accountability.
    C. Privacy by default.
    D. Privacy engineering.

16. A multinational entity needs to analyze sensitive employee data across its global offices without exposing individual information to any unauthorized users. Which privacy-enhancing technology would best allow for secure computation on this data while maintaining privacy across international communications?

    A. Tokenization.
    B. Differential privacy.
    C. Zero-knowledge proofs.
    D. Homomorphic encryption.

17. Tom joined a new social media platform to grow his food catering business. To complete the registration process, he was required to grant the platform permission to access his contact list. Shortly after, his business contacts informed him that they received spam messages from him on loans and insurance products. This is an example of which dark pattern?

    A. Spamming.
    B. Hidden stipulations.
    C. Information milking.
    D. Address book leeching.

18. Which activity will **most** help a controller ensure the operations of a processor are within the scope of the personal data processing agreement?

    A. Privacy audit.
    B. Video surveillance.
    C. Runtime behavior monitoring.
    D. Privacy risk assessment and analysis.

19. Which of the following are required to implement effective privacy engineering?

    A. Data governance, technological controls, engineering life cycle.
    B. Technological controls, entity level controls, business process controls.
    C. Building scalable solutions, enforcement of privacy safeguards, systems design.
    D. Minimization of data, data protection impact assessments, purpose use limitation.

20. Value-sensitive design is an iterative process that involves many types of investigations. Which investigation type focuses on how stakeholders configure, use or are otherwise affected by the technology involved?

    A. Empirical.
    B. Technical.
    C. Conceptual.
    D. Comparative.

21. A company provides training to its employees about customer privacy rights and company privacy policies. The company wants to assess the impact of its training as well as find areas for improvement. Which is the **best** way to evaluate the effectiveness of training in achieving the company's privacy objectives?

    A. Submit questionnaires to training participants after each training, requesting feedback on how the trainings can be made more engaging.
    B. Require team leaders who develop and deliver trainings and refresher courses report to management on which methods are most effective.
    C. Collect information about employees' interactions with customer databases and email correspondences to be reviewed after a complaint has been filed.
    D. Define goals or key performance indicators (KPIs) for the training program and create an audit process for logging and regularly reviewing these KPIs and goals.

22. Identify which of the following is a commonly used threat modelling framework for identifying and evaluating privacy threats in the system development life cycle:

    A. AGILE.
    B. DREAD.
    C. STRIDE.
    D. LINDDUN.

23. Which of the following is a main goal of using the Factor Analysis of Information Risk (FAIR) methodology?

    A. Build an estimate of overall threat.
    B. Create a policy on privacy controls.
    C. Focus on organizational costs and fines.
    D. Develop a strategy for qualitative analysis

24. A tech company's back-office team in India wants to establish a recognition program that rewards "Applause" points as a token of gratitude for the efforts, hard work and dedication that its employees have shown throughout the year. The "Applause" points will be automatically credited to the employee's digital wallet on the employee's birthday. The vendor has asked for employees' names, month and day of birth, work email address, start date, and a profile image, which does not have to be a picture of the employee. An initial file from the HR records has been established to test the setup with the vendor. The test file includes employee name, work email address, work phone number, start date, date of birth, home mailing address, emergency contact name and phone number, and a profile image, all of which the vendor stated were necessary. The privacy team assessing this new process is questioning the data shared for the test. Which of the following is true about the appropriate steps of data minimization when sharing information with the vendor?

    A. Only the requested personal information from the HR system has been shared with the vendor.
    B. The program is in the testing stage, so it is acceptable to include more information than requested.
    C. Excluding, selecting and stripping of personal information from the HR system has not been considered.
    D. The information shared is commonly requested by other vendors, so HR can share it with this new vendor.

SCENARIO II

Please use the following scenario to answer the next TWO questions.

A U.S.-based national retail store chain is looking to expand its business and has recently hired its first chief privacy officer (CPO) and a new chief marketing officer (CMO) to help it drive greater marketing efforts in a way that protects privacy.

The company already operates in several states but currently does not operate in other countries. In addition to its brick-and-mortar retail locations, the company has a website where people are able to order items for home delivery.

The CPO has been asked to review the company's existing practices related to personal data and to remediate any significant issues they identify. One of the first areas that the CPO reviewed was practices related to marketing to existing and potential customers.

The organization used to rely on non-personalized marketing techniques, such as TV and radio advertising and physical billboards, as well as personalized marketing to individuals who have joined their loyalty program. The new CMO is looking to develop and deliver more personalized marketing experiences using personal data to target specific groups and individuals, with the goals of increasing both the customer base and increasing the total amount that existing customers spend per year.

The CMO meets with the CPO and relays that the marketing team has several analyses they would like to run to assist with the marketing efforts:

> First, they would like to identify potential new store locations to meet the needs of online customers who might prefer to shop in-person. The sites must meet the following criteria: (a) they do not have an existing store within 20 miles, and (b) there are a minimum number of people with similar demographics to their existing customers. Before they commence this analysis, they would like to gain a baseline understanding of where their current online customers live.

Second, the CMO would like to run a joint marketing campaign with another company. To do this, they would like to identify customers the two companies have in common so they can target them for this campaign.

After the meeting, the CMO emails the CPO and tells them that as part of their analysis, the marketing team has identified an old customer dataset which has not been updated for several years and does not appear to be in use.

25. Which technique would allow the identification of regular customers to be performed in a way that does not require either company to directly share customers' personal data with the other?

    A. Both companies encrypt their customer lists using asymmetric encryption prior to sharing.
    B. Both companies run each of their customers email addresses through the same hash algorithm and compare the results.
    C. Both companies load the datasets into a single database and only access it through private information retrieval techniques.
    D. The companies set up secure multiparty computation so that neither of them can perform the analysis without the other companies' knowledge.

26. Which of the following actions could the company take with respect to the old customer data set identified by the CMO that will provide the **most** privacy protection?

    A. Delete the dataset after confirming that there is no legal or business reason to retain it.
    B. Email every customer in the dataset to ask whether they would like their data to be deleted.
    C. Strip out any directly identifiable information and then make it available to the analytics team.
    D. Apply access controls to restrict access to just the CMO in the event that a use case is identified.

END OF SCENARIO II QUESTIONS

27. Which of the following is an example of privacy engineering that is focused most specifically on security controls?

    A. Access controls.
    B. Data anonymization.
    C. Data pseudonymization.
    D. Automated data disposal.

28. Which of the following is an example of the predictability objective in privacy engineering?

    A. Enabling users to view their privacy preferences when accessing a website.
    B. Allowing users to make corrections or updates to inaccurate personal data.
    C. Requiring users to check a box stating they have read and agreed to the privacy notice.
    D. Providing users with a contact individual to administer changes to their personal data.

29. Which of the following privacy technologists' activities is recognized as part of the software evolution process?

    A. Analyzing technical log performance data on a regular basis.
    B. Participating in developers' team meetings to discuss new projects.
    C. Assessing the existing privacy controls in the technological ecosystem.
    D. Running a privacy impact assessment when software is being updated.

30. Artificial intelligence can potentially introduce privacy harms to individuals in which of the following ways?

    A. Excluding personal data from collection.
    B. Using personal data in unintended ways.
    C. Hashing data from one set to another set.
    D. Mixing data types to hide relationships among data.

31. To sign up for a retailer's loyalty program, Peter must complete a form asking for his name, contact information, income and other demographic information. Peter completing and submitting the form to the retailer is an example of what type of data collection?

    A. Passive collection.
    B. First-party collection.
    C. Qualitative collection.
    D. Third-party collection.

32. On an annual basis, the tech team performs assessments to evaluate its applications, infrastructure, associated processes and services to ensure regulatory and policy compliance. One of the information protection controls that the team will concentrate on is the application's use of "highly confidential" information in the non-production environments. Application YYZ is in scope for this year's assessment, as a significant amount of confidential personal information (name, home address, date of birth and financial account numbers) is held in the non-production environment. The assessor believes that this presents a risk to the organization, as the controls in the lower environment do not match that of the production environment and, therefore, the personal information is not properly protected. What should the assessor recommend in the report?

    A. The assessor should document this control as compliant, given it is not a deviation of policy.
    B. The assessor should document this control as non-compliant and advise that the policy needs to be updated to include how personal information should be managed in the non-production environments.
    C. The assessor should document this control as non-compliant because the personal information in the non-production environment is classified as "highly confidential."
    D. The assessor should document this control as compliant but advise that the policy needs to be revised to address how personal information should be managed in the non-production environments.

33. A company has hired a marketing company to identify past website visitors who revisit its site for future marketing. This is an example of what type of activity?

A. A digital distraction.
B. A retargeting campaign.
C. A keyword ad campaign.
D. A website personalization.

34. Cody is a software developer who is working on creating a retail website for a company. The company is very dependent on getting as many consumers as possible to sign up to receive marketing. His design team has brought him four different layouts and ideas for a pop-up banner encouraging consumers to sign up for a marketing list. Which of the following design choices would be considered appropriate from a privacy engineering perspective?

A. The pop-up banner offers a discount code for 15 percent off the first purchase if the user provides their email address, but the pop-up banner disappears when the user closes the pop-up using the X.
B. The pop-up banner is central to the screen, even if the user scrolls, and it has no X button to close it. It only disappears if the user interacts with the pop-up by entering their email address.
C. The pop-up banner appears when the user interacts with any other button on the webpage and has two options for the user: The button saying CLOSE is in a blue box and on the left-hand side, and the button saying SIGN UP is in a red box and on the right-hand side.
D. The pop-up banner disappears if the user clicks anywhere outside of the pop-up box or scrolls the page, and it has a clear factual message telling the user that when they sign up, the company will share new deals and promotions with them.

35. A game app available on a popular app store wants to add a requirement for players to include their social media accounts upon signing up. The game app will receive marketing leads from this functionality, and players will get to display their scores and interact with other players. Which of the following would cause a privacy concern?

A. A setting that requires players access the app through the social media account sign-in buttons before playing.
B. A setting that requires users to provide their payment details in the app store if they want to receive daily rewards.
C. A setting that allows signed in players to form and join teams with other signed in players in their area and demographic.
D. A setting that asks players whether the app can use their location services to display their country in the player's profile.

36. Julia decided to reformat her company's website privacy notice. She brought critical elements to the foreground and supplemented those elements with additional related detail to make the privacy notice easier for users to navigate and comprehend. This is an example of utilizing which of the following?

A. Privacy pattern.
B. Clickstream pattern.
C. Data pattern theory.
D. Website design model.

37. An organization is looking to outsource part of its business operations to a third party. As part of the outsourcing, some employees from the third party will require access to the organization's physical locations and some IT systems that contain personal data. Which of the following should an organization do **first** to provide the highest level of security and work to ensure the outsourcing company is granted only appropriate access to personal data?

A. Configure the system's role-based access controls (RBAC).
B. Determine which employees will need access to specific data.
C. Have each individual sign a non-disclosure agreement (NDA).
D. Perform a background check on each employee of the third-party company.

38. Some U.S. states (Illinois, for example) require getting a user's affirmative consent before collecting and using biometric identifiers. Other jurisdictions do not impose this obligation. Developing a national — or global — approach to collection and use of biometrics can be challenging in the face of different legal requirements. The Fair Information Practices (FIPs) can help companies develop their approach. Under which FIP might it be appropriate to obtain consent for collection and use of biometric identifiers?

A. Security.
B. Use limitation.
C. Data minimization.
D. Individual participation.

39. Peart Industries engaged Cheta Security Inc. to perform information security monitoring processes. Cheta Security asked for email addresses of all Peart employees, proposing that if any email activity triggers the security rules, Cheta could share the offending accounts with Peart for investigation. Peart's infosec team offered an alternative solution: each employee could be given a randomly generated user ID when they first receive access to the network. In the event an investigation is triggered, however, the email address would still be recognizable in the company's environment. What data-oriented strategy has been used here to protect the employee's identity?

A. Hiding.
B. Isolation.
C. Obfuscation.
D. Disassociation.

SCENARIO III

Please use the following scenario to answer the next TWO questions.

HomeConnect has made quite a name for themselves in developing a range of smart solution "Internet of Things" technologies which range from remotely controlled security systems to thermostats that can be adjusted from our mobile devices, voice-activated peripherals that allow those less capable of living independently, and other cutting-edge innovations.

They have a very efficient order processing system. Smart devices are configured with default settings and shipped to customers within 24 hours of placing the order. The product box also includes a quick setup guide to save time for the customer. It is not a detailed setup guide, and certain steps, such as changing the password, are assumed to be common knowledge.

It is well known that every instance of the Internet of Things (IoT) in the consumer context will likely become a target to hackers. Compromised IoT devices could expose a vast amount of personal data about an individual's home, work, and health. HomeConnect's cyber-engineering team, in an effort to stay ahead of hackers, often runs real-time updates and patches on endpoints to increase the protection. Whenever a major product release is planned, the team invites interested customers to participate in beta testing to catch failures and usability issues before the final launch.

As part of their overall compliance and risk assessment, HomeConnect ensures that they maintain transparency with individuals about their processing activities to obtain any necessary consent. Despite the security steps taken, a group of hackers were able to access live feeds from the cameras around customers' homes by using a variety of weak, recycled and default credentials. They were even able to communicate using integrated devices. More than thirty families reported that hackers verbally harassed them.

40. What can HomeConnect do to reduce a customer's exposure to threats?

    A. Block the implementation of additional layers of security by the customer.
    B. Require users to change their passwords as part of the initial configuration.
    C. Set up systems to bypass authentication when a customer's home network is not secure.
    D. Advise customers to add household members to their accounts by sharing login credentials.

41. What best practice can the HomeConnect cyber-engineering team adopt for running software updates and patches?

    A. Ensure security patches are delivered over multiple channels.
    B. Inform customers when an update is not ready for implementation.
    C. Notify users when they access the device if there is a software update.
    D. Conduct device vulnerability assessments only after an incident occurs.

END OF SCENARIO III QUESTIONS

42. Information technology has great value across all facets of an organization. Which of the following is a strong business case for holistic data protection, inclusive of privacy, protection and security?

    A. Data protection responsibility should remain with the information technology and information security teams.
    B. Information technology is fundamental to the data life cycle for managing engagement with suppliers and customers.
    C. Collaborative efforts between information technology and other areas of an organization are not a regulatory requirement.
    D. The relationship between information technology and other departments has no true correlation to operational efficiency.

43. Which statement below is **FALSE** with respect to the beta testing of a product?

A. Performed on feature-complete systems.
B. Privacy risks are minimal or non-existent.
C. Open to the broader public but may be capped.
D. Users populate their profiles with personal data.

44. Value-source analysis involves which of the following?

A. Using visual aides to influence and elicit values from stakeholders that will better align with a requisite response.
B. Leveraging narratives or scenarios to identify, communicate, or illustrate the impact of design choices on stakeholder values.
C. Assessing project, designer and stakeholder values and considering the ways in which each group's values may be in conflict.
D. Striving to balance technology and social structure in the design space with a goal of identifying new solutions that might not be readily apparent.

45. Which of the following would be considered part of software vulnerability management?

A. Software testing regime.
B. Software intrusion reports.
C. Software design blueprints.
D. Software developer training.

46. Which of the following is **<u>NOT</u>** an example of the usefulness of conducting a record of processing activity (RoPA) to all types and sizes of organizations?

A. Creating a collated list of personal data from entire book of clients.
B. Identifying who has access to what data and where for supervisory auditing purposes.
C. Classifying sensitive or criminal data to implement data protection policy & procedures.
D. Distinguishing high-risk processing to identify the best solutions to mitigate or manage.

47. Transport Layer Security (TLS) is established using asymmetric cryptography and symmetric encryption and is used primarily to?

A. Protect data in use.
B. Protect data at rest.
C. Protect data in transit.
D. Protect data once received.

48. What must a hiring organization assess while using a third-party service for testing its software?

    A. Whether the service provider has service infrastructure in the cloud.
    B. Whether the service provider has additional services offered at a competitive price.
    C. Whether the service provider has privacy and security equal to or stricter than its own.
    D. Whether the service provider has levels of financial risk tolerance equivalent to its own.

49. What is a primary privacy risk associated with the government's use of facial recognition technology on a public street?

    A. Potential for covert mass surveillance.
    B. Chilling effect on freedom of assembly.
    C. Difficulty in obtaining informed consent.
    D. Increased computational power requirements.

SCENARIO IV

Please use the following scenario to answer the next THREE questions.

During a period of heightened COVID awareness, a large grocery retailer introduced various occupational and customer-related health and safety initiatives in their stores to help reduce virus spread and increase the ability to contact trace. One such initiative was to ask that all customers entering their physical stores provide their names, email addresses and/or mobile phone numbers. The prescribed method to enable this was through a ballot-box system, where prior to entering a store, customers would complete appropriate forms and then submit them into a secured ballot-box. However, some stores were struggling to keep up with customer demand, and in the interest of expediency, simply provided paper forms on clipboards outside their stores for people to complete. Each new customer would append their details below the previous customer with the details being publicly visible.

The retailer's customer service center received a call from a customer complaining that she was contacted by someone she didn't know. The man stated he had obtained her information from a list outside one of the stores she visited. He said he would only delete her information if she agreed to meet him in person; otherwise, he would post her personal data on social media.

50. Which of the following privacy threats and violations is the man's action an example of?

    A. Blackmail.
    B. Accessibility.
    C. Surveillance.
    D. Appropriation.

51. Which type of privacy threat and violation did the retailer enable through unsecured lists outside its store?

    A. Dark patterns.
    B. Digital profiling.
    C. Specific surveillance.
    D. Increased accessibility.

52. If the store that adopted this questionable practice also used the list to engage in email or SMS marketing to customers, what type of privacy threat and violation would this be?

    A. Intrusion.
    B. Insecurity.
    C. Data misuse.
    D. Interrogation.

END OF SCENARIO IV QUESTIONS

53. Which of the following is an example of the use of a privacy pattern?

    A. A common recurrence of privacy law violations within a company.
    B. An organization's color scheme within their privacy policy documentation.
    C. A preformatted response to similar privacy-related inquiries received on a website.
    D. A phone app feature which reminds the user that their location data is being shared.

54. Which of the following protects information while it is in use by multiple parties?

    A. Using Secure Multiparty Computation application.
    B. Using password to protect a Microsoft Word document.
    C. Using URL that begins with https:// when accessing a website.
    D. Using WPA2 wireless network protocol for free public internet access.

55. Other than when new privacy laws or regulations are enacted, how often, at a minimum, should an organization update its privacy standards to ensure they are meeting expectations and requirements?

    A. Annually.
    B. Quarterly.
    C. Bi-annually.
    D. Semi-annually.

56. To prevent the identity of employees from being exposed when analyzing data for potential automation opportunities, the compliance team requires that information captured to perform capacity diagnostics on employee screen time usage be?

    A. Perturbed.
    B. Correlated.
    C. Summarized.
    D. Disseminated.

57. Which of the following would be an indication of effective privacy engineering?

A. The organization implemented a card data environment perimeter and passed its PCI audit.
B. The IT department implemented automated user account provisioning by using single sign-on.
C. The organization implemented proactive privacy measures in its software development life cycle.
D. The marketing department updated the company's privacy policy to include information on biometric identifiers.

58. BitHealth has recently implemented an electronic medical record (EMR) system. All patient information is now stored in the EMR. Only those who have gone through an approval process by the privacy team have access to the EMR. Lea, a member of the BitHealth IT team, has received a request from Stony Surgery requesting access to the EMR so its case management team can approve/authorize inpatient interactions. How should Lea respond to the request from Stony Surgery?

A. Delete the email at once as it could be a phishing attempt.
B. Forward the request to the privacy team at BitHealth to respond.
C. Provide access to Stony Surgery because it is a health care provider.
D. Request a signed letter from a senior member of the practice to verify authority.

SCENARIO V

Please use the following scenario to answer the next FIVE questions.

EdMed Inc. is one of the largest U.S. digital training companies fulfilling educational needs of many of the world's health care professionals. Using high-resolution interactive video, they provide the finest educational experience, focusing on the secure and effective use of real-life surgery recordings for state-of-the-art medical products and techniques.

Recently, the customer care department received a notice from the American Hospital surgical team in Rome, Italy about post-operation details found in certain case study educational materials. They included the patient's name and Massachusetts Official Hospital details on an x-ray that was shown on video as a part of the EdMed Inc. training set.

EdMed's privacy network expert team reviewed the content. They then organized an urgent meeting with all stakeholders—Mark, Peter and Jane—to evaluate the risk of the incident and to analyze how to avoid this situation in the future.

Mark and Peter are both privacy technologists responsible for acquiring and preparing raw data collected from different hospital sources by following EdMed's privacy-by-design process. Jane is a project manager from TristarGlobe Inc., a specialized media company that develops training materials on behalf of EdMed Inc.

Mark uses internally developed software, called DONAT, to parse the raw data collected and to identify any personal data that should be removed from training materials before they are released to the market. Peter then forwards raw data, including a change notice, to Jane, who then manages the production and release of the final training materials.

Jane determines that they had received the x-ray containing personal data but there was no request to remove any details from it. Mark confirms that there was no change notice sent for the x-rays because Massachusetts Official Hospital is using a new x-ray format that was not recognized by DONAT.

Mark, Peter and Jane all agree TristarGlobe Inc. must take a more proactive role to determine the least amount of personal data needed on the training materials. Peter also proposed a DONAT request for change notice that will introduce an auditability quality attribute, which will have the ability to examine and review how the system parses raw data during production. These new procedures will require approval from additional stakeholders to provide an appropriate budget, staff, and additional approvals for the process, as well as proper training for those affected by the new procedure.

Mark reported feedback from the legal department indicating that the case study materials constituted a data breach and that they have no documented output of a privacy risk assessment in this situation. They discuss meeting with the appropriate team members to develop privacy risk assessments for all processes that potentially involve personal data moving forward.

Closing the meeting, all three agree that they must enforce any new processes and demonstrate that all parties involved are compliant with privacy policies and processes in the future.

59. To help Jane to take a more proactive role and to comply with standards, Peter and Mark will need to send her standard operating procedures (SOP) covering which of EdMed's privacy-by-design process activities?

    A. Raw data testing and validation SOP.
    B. Identify training information needs SOP.
    C. Documenting training requirements SOP.
    D. Low-level design and implementation SOP.

60. The type of requirement that Peter proposed related to the upgrade of the technological system that parses the raw input data for TristarGlobe Inc. processing is known as what?

    A. A functional requirement.
    B. An exclusion requirement.
    C. A predictability requirement.
    D. A nonfunctional requirement.

61. Following the report from the legal department, Mark should require which of the following be performed?

    A. Legal impact assessment.
    B. Privacy impact assessment.
    C. Transfer impact assessment.
    D. Legitimate impact assessment.

62. Which control will be used to implement the final statement on which Peter, Mark and Jane agree?

    A. Balance.
    B. Security.
    C. Supervision.
    D. Architecture.

63. Peter and Mark's first step was to collect all the facts about the reported situation, which included software, procedures and vendors. What is this process known as?

    A. Privacy audit and IT control review.
    B. Penetration test reporting and analysis.
    C. Incident response procedure and review.
    D. Data protection gap and process analysis.

END OF SCENARIO V QUESTIONS

64. David is the privacy technologist at an EU company that has decided to use legitimate interest as the lawful basis for processing the personal data of its customers in the new fraud prevention solution the company is developing. Following privacy by design principles, David proposed an assessment that will document the legitimate interests, ensuring transparency and fairness of data processing. Which of the below concepts is the **most** appropriate control David should propose?

    A. Balance.
    B. Supervision.
    C. Assessment.
    D. Architecture.

65. Which of the following would be considered a type of privacy interference?

    A. Installing closed circuit television cameras on public streets.
    B. Providing credit history that leads to inaccurate credit scores.
    C. Completing an employment application truthfully and accurately.
    D. Submitting an email address to receive a marketing email newsletter.

66. Which of the following scenarios **best** describes a situation where there could be surveillance without the reasonable knowledge of the individual?

    A. A review platform discloses users' identities rather than allowing for anonymity when providing reviews.
    B. An airport uses heat sensing cameras to screen individuals for fever while individuals pass through security checks.
    C. A regulator reviews the financial transactions of individuals who have been placed on a government sanctions list.
    D. A website matches the user's IP address and browsing pattern to registered users regardless of whether the user is logged in.

67. Which of the following **best** describes the goal of privacy engineering?

    A. To ensure that all personal data is completely anonymized within a system.
    B. To develop privacy-protective solutions that are in line with the business' needs.
    C. To ensure that data collection practices are aligned to an appropriate legal basis of processing.
    D. To ensure that solutions appropriately protect confidential data in accordance with company policies.

68. A data broker collects information on medications that are prescribed to individuals and sells this information to pharmaceutical companies to allow them to target their advertising budgets. The information they collect does not contain direct identifiers regarding the individuals to whom the medications are prescribed, but does contain several indirect identifiers that in combination could allow reidentification. What must the data broker do prior to selling this data to pharmaceutical companies?

    A. No action is necessary prior to selling this data.
    B. The data broker is not allowed to sell this data set.
    C. The data broker must anonymize the data set before it can be sold.
    D. The dataset must have a k-anonymity value greater than eighteen before it can be sold.

69. The leadership team for a retailer wants to improve customer satisfaction and increase customer retention. They propose introducing software that would enable them to learn more about their customers' attitudes and behaviors to act upon. Their IT team is leading efforts to select a closed-source loyalty management system for this purpose by creating a list of software requirements and undertaking a tender process. These requirements include ensuring robustness of software against attack and vendor support for patching and customizations. Which is the following is **TRUE**?

    A. A closed-source loyalty management system has easily viewable code.
    B. A closed-source loyalty management system can only be fixed by the vendor.
    C. A closed-source loyalty management system has code that is regularly shared and modified.
    D. A closed-source loyalty management system by its very nature is more resistant to attack than open-source.

70. Which of the following controls would best help a company maintain compliance when the software development cycle moves into the product release stage?

    A. A rule that any applied code change, upgrade or patch will generate an email alert to the privacy compliance subject matter expert.
    B. A set of change control standard operating procedures that require any significant privacy changes to be reviewed by a cross-functional team.
    C. A privacy compliance subject matter expert proactively reviews all software assets every quarter to monitor whether there have been any changes.
    D. The software is subject to an internal data protection audit, which will review whether the software is as described in its release notes, conducted on a two-year cycle.

71. A company wants to build a brand image that differentiates itself from the competition by focusing on enhancing customer trust to grow its business. In the company's online environment, they want to empower data subjects to play an active role in the management of their own data, via a consent mechanism. Which of the following privacy by design foundational principles **best** supports this initiative?

    A. Full functionality – allow users full access.
    B. End to end security – full life-cycle protection.
    C. Respect for user privacy – keep it user centric.
    D. Proactive not reactive - preventive not remedial.

72. Software that collects and reports runtime failures to a bug tracker may sometimes include the user's personal data as part of the bug report. What should be a design consideration for such automated bug trackers?

    A. Transmit user's personal data without explicit disclosures.
    B. Publish the bug report online with the user's personal data.
    C. Encrypt personal data during transmission and after receipt.
    D. Duplicate the entries in the bug report, including the personal data.

SCENARIO VI

Please use the following scenario to answer the next TWO questions.

You have just been hired by Hybrid-Co as their technical lead for workplace resources (WPR) and human resources IT systems. In Spring 2020, all workers were sent home due to the COVID-19 pandemic and only remote work was permitted. As the pandemic moved into an endemic phase, hybrid work quickly became the norm (i.e., some workers are in the office and others are remote). You were tasked with designing the company's hybrid work model and leading the company-wide initiative for employees to return to the office safely.

The first task the CEO asked your team to complete was to assess how much office space was needed to provide sufficient workspace for employees who want to work in an office environment. Relying on your own experience and the team's expertise, you design a system that combines information from security logs from badge readers, Wi-Fi access point logs, and video footage from CCTV security cameras to collect information about people who enter and exit into the building and connect their devices to the company's Wi-Fi. This data is de-identified and aggregated to protect individual privacy.

While the pandemic was moving toward an endemic phase, periodic COVID-19 surges still occurred. Hybrid-Co had to take steps to make the office environment as safe as possible. In that regard, the chief medical officer asked you to help devise a method to track COVID-19 positive cases in the office.
With so many remote workers in the new hybrid work environment, managing by walking around is not as effective as it used to be, and managers have rising concerns about employee productivity. For your third task, you were asked to assess what tools, logs, information and metadata were available to measure productivity and employee engagement within the hybrid work model.

73. Do the company's data collection processes regarding building access align with the OECD Fair Information Practices and Ann Cavoukian's Privacy by Design framework?

    A. Yes, the company has a right to use non-personal data in its possession to further legitimate business objectives.
    B. Yes, provided the company obtains explicit, written consent from the data subjects to utilize the de-identified data.
    C. Yes, as long as the data is used to determine which specific employees need access on certain days to provide appropriate workspaces.
    D. Yes, provided only the IT team can reidentify individuals from the data collected and it is used for facilities management, a reasonably anticipated secondary use.

74. Which of the following did you neglect to do in your haste to comply with your CEO's request?

A. Obtain employee explicit consent prior to engaging in any monitoring of their activities.
B. Ensure you do not monitor employees' productivity to avoid breaking their trust and invading privacy.
C. Consult with the legal department to ensure compliance with all applicable laws and regulations.
D. Evaluate whether the processes ensure employees' productivity and the company's profitability.

END OF SCENARIO VI QUESTIONS

75. In the privacy by design model, imposing controls within a design system reduces threat actors' access to personal information and minimizes privacy risks when collecting or processing personal information. Which of the following is an example of a security control?

A. Using pseudonymous data and then pushing that data toward a user-centric architecture.
B. Allowing full access to all detailed information available to specific users in the system based on users' locations.
C. Summarizing detailed information into categories based on more abstract attributes and restricting access to summary information.
D. Using internal privacy policies for each department that best describe how the organization wishes to manage and protect personal information.

76. Industrial Industries, Inc. collects customer personal data to assist with product returns. Three years after the sale, customers can no longer return the product, but Industrial Industries wants to continue using some of this information to analyze the percentage of returns during that period of time. Of the following optons, which is the **best** practice to mitigate risks associated with maintaining this data for return analyses?

A. Review the information collected in the database and delete any personal data that could be used to identify customers.
B. Review employee access levels for the database and remove those individuals who no longer have a business need to access the information.
C. Develop an automated process that removes the customer's email address from the database and avoids human error when deleting that information.
D. Save unneeded customer personal data in a distinct database that has additional security measures, such as enhanced authentication requirements.

77. You work in human resources and want to deploy a new tool that will assist with recruitment through the use of AI. Which of the following actions is **least likely** to eliminate bias/discrimination when using this tool?

A. Focusing on inputs and outcomes of the AI tool.
B. Asking the recruit if they think the outcome is fair.
C. Regularly auditing the algorithms to ensure fairness.
D. Having humans review decisions made by the tool.

78. Which of the following IT roles serves as a repository of privacy knowledge and tailors this knowledge as needed to help different stakeholders fulfill their roles?

A. Area specialists.
B. Project managers.
C. Process administrators.
D. Software programmers.

79. Which of the following is a tool that shows the relationship between the requirements of a privacy law and the implemented software design elements?

A. Digital signature.
B. Traceability matrix.
C. Block level disk encryption.
D. Cryptographic hash function.

80. Linda visits a website to register as a paid test subject for a cancer research project for the first time. Besides her contact information, she is required to provide extensive health information about herself and family members. Clicking on the link that explains how the health information will be used, Linda is directed to a long and verbose medical statement that she does not understand. This is an example of which privacy pattern?

A. Fair distribution reciprocity.
B. Abridged terms and conditions.
C. Minimal information asymmetry.
D. Medical information asymmetry.

81. Which of the following is an example of a privacy threat during data collection?

A. A credit card payment processor monitoring each transaction as it occurs.
B. An employer asking an interviewee about marital status during a job interview.
C. A doctor adding auxiliary information to a patient's record during a consultation.
D. A credit bureau aggregating an individual's payment history from multiple creditors.

82. As part of a major rebranding effort, a social media company is adding new features to its mobile app, including embedded application programming interfaces (APIs) that easily give users access to other social media services. Before rolling out these changes, what should the company's privacy team do?

A. The company should develop an email and social media marketing campaign targeting existing customers to make them aware of these features.
B. The company should assess if the inclusion of the APIs alters the way current customer's data is used and notify those customers of those changes.
C. The company should select a group of current customers for a beta test and confirm there are no conflicts with the core product before sending out notice.
D. The company should create a new privacy policy and notify current customers of new features and provide links to descriptions of the technologies being used.

83. Which security mechanism would be the **most** reliable technology to keep data confidential at rest, in-transit, or when processing real-time analytics?

    A. Data backup.
    B. Data encryption.
    C. Hardware-based security.
    D. Two-factor authentication.

84. Which of the following events is a trigger to update a data protection impact assessment or privacy impact assessment (DPIA/PIA) for a system?

    A. The organization merges with a competitor.
    B. The organization patches its operating system.
    C. The organization hires a new chief privacy officer.
    D. The organization acquires a new office space in the same city.

SCENARIO VII

Please use the following scenario to answer the next FIVE questions.

Shop4Electronics, a large electronics retailer has a website and a mobile app where its customers can make purchases, see their order history and start returns.

Shop4Electronics uses a variety of tracking technologies on its website and app.
The Shop4Electronic website uses several pieces of web code that in turn leverage cookies for the purposes of internal analytics, fraud detection and digital advertising.

When a user visits the Shop4Electronics website they are assigned several different cookie IDs. The code on the website collects the cookie ID of each user and associates that data to any completed purchases together with any browsing behavior on the website. In addition, information about the user's device is collected and associated to their cookie IDs. This information includes their IP address, device operating system, device type, browser name, screen size, browser language and list of browser plugins installed.

A user visits the Shop4Electronics website and completes an order for two new laptops. The user later receives an email that their order was rejected as their fraud vendor, FraudNoMore, marked the transaction as fraudulent.

FraudNoMore uses their third-party cookie IDs collected from the Shop4Electronics website and associated device data described above to make their determination of fraud. However, if their third-party code is unable to set and collect cookies and other device information about the user, it automatically considers that transaction fraudulent.

In addition to the website, the Shop4Electronics mobile application uses the browsing behavior of its users for the same set of uses cases as their website. The use cases are analytics, fraud detection, and digital advertising.

To deliver digital advertising, the Shop4Electronics mobile app collects the mobile adverting identifier in combination with the browsing activity and sends that data to its social media and advertising partners. Those social media and advertising partners in turn use those mobile advertising identifiers to serve digital advertisements for Shop4Electronics.

A user downloads and installs the Shop4Electronics Mobile App to their new iPhone. Upon opening the app, Shop4Electronics asks for permission to track the user via the Apple-provided App Track Transparency (ATT) dialog, which requires consent. This dialog is required to access the advertising identifier on any iPhone or iPad running iOS 14.5 or later. The user rejects the request to be tracked by selecting 'Ask App Not to Track' in the dialog. Despite declining to be tracked, the user can use to app as normal.

85. There has been an increase in calls to the customer service department of Shop4Electronics with complaints that orders were rejected incorrectly due to fraud. Which recommendation should be provided to reduce the number of false positives identified by FraudNoMore?

    A. Disable FraudNoMore entirely as fraud detection is not a valid business reason to track users.
    B. Ask users to reset cookies in their browser and try again if their transaction is rejected as fraudulent.
    C. Stop marking transactions as fraudulent when third-party code is unable to set cookies and collect associated data.
    D. Require all users to have a unique IP address when making a purchase to avoid matching a known fraudulent IP address.

86. If a guest visitor on the Shop4Electronics website cleared their cookies, which technique could be used to continue to uniquely identify that user, based on the data collected by Shop4Electronics and its partners?

    A. Federated Identity.
    B. Anthropomorphism.
    C. Cross-site Scripting.
    D. Device Fingerprinting.

87. A Shop4Electronics customer signs-up to receive email marketing. This customer is concerned about privacy and wants to take steps to ensure Shop4Electronics is not notified when they open a Shop4Electronics email. Which method would limit email open tracking?

    A. Use of an email client that blocks images and execution of specific scripts.
    B. Installing an ad blocker on each browser the customer uses on all devices.
    C. Disable location tracking in the Shop4Electronics mobile app and on all browsers.
    D. Use of a virtual private network (VPN) service to access email and Shop4Electronics' website.

88. The Shop4Eletronics website requests a user's location via their browser upon first visit to the site. This location data is used to determine a zip code to calculate shipping cost and tax. Upon navigating to checkout, the user notices their zip code has been pre-populated. Which mechanism was likely used to determine location if the user rejected to share location via their browser?

    A. Location from GPS data.
    B. Location from IP address.
    C. Location from MAC address.
    D. Location from advertising ID.

END OF SCENARIO VII QUESTIONS

89. Your company is contemplating deploying an app that tracks users' specific locations and sells that information to third-party advertisers. Which of the following is the final concern of those listed that will need to be addressed?

   A. The extent to which the users' information is compiled into a profile.
   B. The extent to which the location might track someone to a "sensitive" place.
   C. Whether individuals have been provided sufficient notice of the tracking activities.
   D. Whether the agreement with the developer is compliant with your privacy policies.

90. In the context of a large supermarket chain, which of the following actions best demonstrates support for individuals' privacy rights requests?

   A. Sharing customer data with third-party vendors routinely to improve service offerings.
   B. Limiting personal data processing to only what is necessary for completing transactions.
   C. Allowing customers to access and correct their personal data through a secure online portal.
   D. Storing all customer purchase histories permanently to personalize future marketing campaigns.

Answer Key

For each correct response, place a “1” or a checkmark in the corresponding domain column (white box).
Note: Domains are indicated by an unshaded (white) box. Competencies are noted in the blue columns.

Item Number	Correct Answer	Domain I	*Competency*	Domain II	*Competency*	Domain III	*Competency*	Domain IV	*Competency*	Domain V	*Competency*	Domain VI	*Competency*	Domain VII	*Competency*
1	**C**		*B*												
2	**A**						*D*								
3	**D**						*D*								
4	**A**						*D*								
5	**C**						*F*								
6	**D**				*B*										
7	**B**												*A*		
8	**A**								*C*						
9	**D**		*D*												
10	**D**						*B*								
11	**B**		*A*												
12	**B**										*D*				
13	**A**										*A*				
14	**C**						*E*								
15	**A**		*B*												
16	**D**														*E*
17	**D**												*C*		

Item Number	Correct Answer	Domain I	*Competency*	Domain II	*Competency*	Domain III	*Competency*	Domain IV	*Competency*	Domain V	*Competency*	Domain VI	*Competency*	Domain VII	*Competency*
18	**A**										*C*				
19	**A**												*B*		
20	**A**										*C*				
21	**D**		*C*												
22	**D**												*A*		
23	**A**		*A*												
24	**C**								*A*						
25	**B**								*C*						
26	**A**								*C*						
27	**A**												*A*		
28	**C**												*B*		
29	**D**		*C*												
30	**B**														*D*
31	**B**		*D*												
32	**D**										*D*				
33	**B**														*B*
34	**D**												*C*		
35	**A**		*D*												
36	**A**										*B*				
37	**B**								*C*						
38	**D**						*A*								

Item Number	Correct Answer	Domain I	*Competency*	Domain II	*Competency*	Domain III	*Competency*	Domain IV	*Competency*	Domain V	*Competency*	Domain VI	*Competency*	Domain VII	*Competency*
39	**C**								*A*						
40	**B**														*A*
41	**C**										*B*				
42	**B**		*C*												
43	**B**										*B*				
44	**C**				*A*										
45	**B**						*E*								
46	**A**		*C*												
47	**C**								*C*						
48	**C**				*A*										
49	**A**														*C*
50	**A**						*D*								
51	**D**						*C*								
52	**C**						*C*								
53	**D**												*C*		
54	**A**						*D*								
55	**A**		*C*												
56	**C**														*D*
57	**C**												*A*		
58	**B**				*A*										
59	**B**										*A*				

Item Number	**Correct Answer**	**Domain I**	*Competency*	**Domain II**	*Competency*	**Domain III**	*Competency*	**Domain IV**	*Competency*	**Domain V**	*Competency*	**Domain VI**	*Competency*	**Domain VII**	*Competency*
60	**D**										*A*				
61	**B**		*C*												
62	**C**										*A*				
63	**C**						*B*								
64	**A**												*D*		
65	**B**						*E*								
66	**D**						*B*								
67	**B**												*B*		
68	**C**								*C*						
69	**B**						*E*								
70	**B**												*D*		
71	**C**		*A*												
72	**C**						*B*								
73	**A**		*B*												
74	**C**														*D*
75	**C**												*D*		
76	**A**								*A*						
77	**B**						*A*								
78	**A**				*A*										
79	**B**								*B*						
80	**C**												*C*		

Item Number	Correct Answer	Domain I	*Competency*	Domain II	*Competency*	Domain III	*Competency*	Domain IV	*Competency*	Domain V	*Competency*	Domain VI	*Competency*	Domain VII	*Competency*
81	**B**						*B*								
82	**B**								*B*						
83	**B**								*C*						
84	**A**				*B*										
85	**C**														*B*
86	**D**														*B*
87	**A**														*B*
88	**B**														*B*
89	**D**						*B*								
90	**C**				*B*										
SUMMARY		**___ of 15 correct**		**___ of 7 correct**		**___ of 20 correct**		**___ of 12 correct**		**___ of 11 correct**		**___ of 14 correct**		**___ of 11 correct**	
PERCENTAGE (# correct/# total) x 100															

Item Rationales

1. The correct answer is C. Embedding privacy controls into each stage of the data processing life cycle from collection to destruction ensures comprehensive protection of customer data, aligning with Privacy-by-Design principles. This reflects the principle of end-to-end security and full life cycle protection, which is a core aspect of Privacy by Design.
   Body of Knowledge Domain I, Competency B

2. The correct answer is A. Dark patterns are programming techniques which are intended to misguide or deceive website users. This is the opposite of privacy patterns, which are programming techniques intended to maintain or enhance an individual's privacy rights. In this example, the website designer used a dark pattern technique to heavily influence and trick Jenny to make a certain choice. A data controller needs to ensure that users can properly inform themselves before making a choice. Otherwise, processing their information may be unlawful in some jurisdictions because consent is invalid. Unfortunately, providing two inferior choices resulted in Jenny's uninformed consent to receive targeted advertisements on the company's website.
   Body of Knowledge Domain III, Competency D

3. The correct answer is D. Aggregating data can be a good way to protect information about individuals. However, a variety of methods, such as statistical analysis or comparison to other databases, can permit the recreation of underlying data and identify individuals.
   Body of Knowledge Domain III, Competency D

4. The correct answer is A. There are likely to be people with the same last name at an address and it is not always the case that the main bill payer has the most active credit history. The application of this rule could lead to an individual being falsely identified as the main utility account holder and cause a distortion of their credit score if the debts are attributed to them. When combining data or linking data, the logical rules used to make matches must be vigorously tested to prevent distortion of data sets and negative consequences for individuals.
   Body of Knowledge Domain III, Competency D

5. The correct answer is C. Organizations have huge investments in their software systems—they are critical business assets. To maintain the value of these assets to the business, they must be changed and updated. Most of the software budget in large companies is devoted to changing and evolving existing software rather than developing new software. A spiral model of development and evolution represents how a software system evolves through a sequence of multiple releases. The process of software evolution is driven by requests for changes and includes change impact analysis, release planning and change implementation. However, the concerns of the development team should extend beyond functionality to include the impact the changes have on the personal data the company processes. Advances in technology used to process personal data and an increase in privacy legislation have created a need for software to be more secure and privacy compliant.
   Body of Knowledge Domain III, Competency F

6. The correct answer is D. A data protection impact assessment (DPIA) is a privacy compliance tool introduced by the GDPR that can test potential privacy and data protection issues at all phases of a product life cycle. The process of conducting a DPIA includes identifying risks and exploring ways to mitigate or manage those risks.
   Body of Knowledge Domain II, Competency B

7. The correct answer is B. To conduct a privacy risk assessment, an organization will need to know, among other things, what data the company has collected and maintains in its systems before it can determine the privacy risks around that data. For example, in addition to knowing what data the company has, it will also need to know the purposes for which the data is being used.
   Body of Knowledge Domain VI, Competency A

8. The correct answer is A. Careful risk analysis must be done to ensure that data sets have been truly anonymized. Removal of direct identifiers is a suppression method that is effective but must be considered in conjunction with other techniques. Seemingly nonidentifiable attributes can be combined to identify an individual even when the direct identifiers are removed. Generalization is another technique to improve the anonymity of data, but it also has limitations. Age can still be a uniquely identifiable attribute in the data set depending on the context, e.g., the individual could still be the oldest or youngest individual in the data set and thus identifiable. Removing outliers in the data sets, either by generalization or noise addition, is a good technique but also is not effective in isolation because there may be another unique attribute.
   Body of Knowledge Domain IV, Competency C

9. The correct answer is D. Implementing a strict data retention policy that automatically deletes customer data after a specified period unless retention is legally required ensures that data is not kept longer than necessary, aligning with privacy principles. This reflects the principle of data minimization and proper data retention management, which are crucial for demonstrating compliance with privacy principles during the data life cycle.
   Body of Knowledge Domain I, Competency D

10. The correct answer is D. The company has made representations to existing users that their information would remain private. To now reveal that information would be a material change from the original representations made to users, and moving forward would be viewed as violating privacy laws around the globe.
    Body of Knowledge Domain III, Competency B

11. The correct answer is B. By giving individuals the ability to mask their identities, the company provides people with choice about what information is publicly available on the website when they post a review.
    Body of Knowledge Domain I, Competency A

12. The correct answer is B. A compensating control is a short-term control that reduces the risk of personal data exposure when the technical or organization measure is unavailable, which in this case, is a delay in the installation of the quick-fix to the vulnerable CRM system. The compensating control must also not impact the business and at the same time, provide assurance that risk is managed.
    Body of Knowledge Domain V, Competency D

13. The correct answer is A. Many data-driven organizations collect data first and find uses for it afterward. Implementing privacy by design through minimization requires understanding what information is required to accomplish a goal and limiting the collection to only that.
    Body of Knowledge Domain V, Competency A

14. The correct answer is C. The bank's policies are driven by critical regulatory requirements and will determine the safe and acceptable use (or not) of open-source software. The policy may dictate what sources and license type are acceptable for use as guidance for the DevOps team before other downstream activities such as risk/benefits analysis should take place.
    Body of Knowledge Domain III, Competency E

15. The correct answer is A. The concept of "visibility and transparency" is one of Dr. Ann Cavoukian's seven foundational privacy principles of Privacy by Design. This principle focuses on being open about the use of personal data and ensuring that the disclosure about the use makes sense to the data subjects and other relevant stakeholders.
    Body of Knowledge Domain I, Competency B

16. The correct answer is D. Homomorphic Encryption allows computations to be performed on encrypted data without decrypting it. This technology enables the corporation to analyze aggregated employee data across offices while maintaining individual privacy. It's particularly suited for scenarios involving sensitive data transmission and processing across international boundaries, addressing both privacy and compliance concerns in global communications.
    Body of Knowledge Domain VII, Competency E

17. The correct answer is D. Leeching is a social media process wherein information is gathered for one purpose and then used for another. The social media company urged Tom to share his contacts to access a site function. The information was then used for unauthorized purposes such as spamming his contacts with information in Tom's name.
    Body of Knowledge Domain VI, Competency C

18. The correct answer is A. Auditing provides visibility into processes and recognizes the gap between what one should do to protect privacy and the actual practices. To maintain accountability, the data controller must provide regular vendor audits to detect if there is any violation of the data processing agreement or the technical and organization measures agreed upon.
Body of Knowledge Domain V, Competency C

19. The correct answer is A. Privacy engineering requires the incorporation of effective data governance, as well as technical controls, and embedding of privacy consideration within the engineering life cycle to be holistically effective.
Body of Knowledge Domain VI, Competency B

20. The correct answer is A. Empirical investigations are qualitative or quantitative investigations that attempt to understand the various stakeholders and their values, as well as any value conflicts that may arise. Conceptual investigations identify direct and indirect stakeholders, attempts to establish whatever stakeholders may value and determines how stakeholders are impacted by design. Technology investigations examine how existing technologies support or hinder human values and how the technology might be designed to support the values identified during the conceptual investigation. Comparative investigations are not a type of value-sensitive design investigations.
Body of Knowledge Domain V, Competency C

21. The correct answer is D. A good logging and audit process allows organizations to demonstrate compliance with privacy obligations and identify and respond to deviations. However, merely logging information is not sufficient; an organization must at least periodically review logs. Logging can collect information about both technical (e.g., logins, account changes) and non-technical (e.g., customer complaints, number of phone calls) events. Auditing this information provides visibility into the company's risks and the effectiveness of risk management.
Body of Knowledge Domain I, Competency C

22. The correct answer is D. LINDDUN is a recognized privacy threat modeling framework, developed by privacy experts at KU Leuven. It offers support to identify and mitigate privacy threats early in the development life cycle. It helps you identify potential privacy threats based on the 7 key LINDDUN threat types: Linking, Identifying, Non-repudiation, Detecting, Data Disclosure, Unawareness, Non-compliance. STRIDE and DREAD are both security threat models so are often used in tandem with LINDDUN. AGILE is a project management methodology used by many software developers to be able to manage projects quickly.
Body of Knowledge Domain VI, Competency A

23. The correct answer is A. Factor Analysis of Information Risk (FAIR) is a quantitative risk methodology for information security risk. The purpose of FAIR is to identify factors that can be calculated or reasonably estimated, thereby building an estimate of overall threat or risk. It is not the goal of FAIR to have precision or certainty, but rather a logical and defensible range related to risk.
    Body of Knowledge Domain I, Competency A

24. The correct answer is C. Excluding, selecting and stripping of personal information from the HR system has not been considered. The goal is to share the least amount of personal information required to perform the process. Date of birth includes the year, which was deemed not necessary by the vendor. Additionally, emergency contact, emergency contact's phone number and profile image are not required for the vendor to deposit 'Applause' points into the employees' digital wallets.
    Body of Knowledge Domain IV, Competency A

25. The correct answer is B. By first hashing all the email addresses and then comparing the results, each organization could understand the overlap in the datasets that represented common customers without sharing any of the other customer information.
    Body of Knowledge Domain IV, Competency C

26. The correct answer is A. The most privacy protective measure is to delete the dataset. Data minimization includes deleting or destroying data that is no longer in use, which reduces the risk of harm to consumers and the risk to the organization in the event of a breach or incident.
    Body of Knowledge Domain IV, Competency C

27. The correct answer is A. Security measures such as encryption, access controls, and regular audits help bolter privacy engineering efforts. Data anonymization, data pseudonymization, and automated data disposal are privacy engineering controls, but not specifically security controls.
    Body of Knowledge Domain VI, Competency A

28. The correct answer is C. Predictability characterizes reliable assumptions about a system, particularly its data and the processing of that data by all stakeholders. Measurable events such as user participation in acknowledging and agreeing to the privacy notice, will eliminate surprises during later phases of the system use provided the privacy notice is correct, enabling the predictability objective to be met.
    Body of Knowledge Domain VI, Competency B

29. The correct answer is D. When software that processes or contains personal data is being updated or changed, it is critical that a privacy impact assessment is performed on the proposed changes or updates. Changes to how a software operates could significantly change the collection of, access to, or other processing of personal data. Ensuring the software changes do not negatively impact personal data is a key function of the privacy technologist and to the software evolution process.
Body of Knowledge Domain I, Competency C

30. The correct answer is B. Privacy harms can be introduced when data is processed in unintended ways. Artificial intelligence could potentially introduce tasks or processes that manipulate data to influence people's buying choices.
Body of Knowledge Domain VII, Competency D

31. The correct answer is B. First-party collection happens when the data subject provides information about themself directly to the collector and is generally the most accurate of collection methods. As with any personal data, however, it is critical that those collecting the data only collect what is necessary for the purpose and delete the data once it is no longer needed.
Body of Knowledge Domain I, Competency D

32. The correct answer is D. Personal information in the lower environment should be protected using the same controls as in the production environment, or to the industry standard, but neither are in place. The information protection policy needs to be revisited to assure that personal information is contemplated.
Body of Knowledge Domain V, Competency D

33. The correct answer is B. The term "retargeting" refers to online advertising campaigns where the advertiser attempts to get website visitors to come back to the company's website. The campaign works by dropping a cookie on the user's computer. When the user leaves the site, the cookie identifies that user and allows them to be served with ads encouraging their return to the website.
Body of Knowledge Domain VII, Competency B

34. The correct answer is D. Options A-C are examples of dark patterns that manipulate or force the user to provide their personal data to use the service or purchase the goods provided by the website. Privacy engineers must resist any attempts to insert deceptive design into websites, such as reversal of color and position of buttons (in the west most people associate green with good, red with bad, or grey with close and most people expect Yes and No in that order left to right on the page). Offering discounts is also considered a dark pattern since it is asking the user to give up their privacy rights in return for a reward. Websites that deliberately try to generate user frustration by not allowing them to see past the pop-up banner are also using dark patterns to annoy the consumer into consenting to data collection.
Body of Knowledge Domain VI, Competency C

35. The correct answer is A. A sign-up screen that does not permit you to enter the game without providing additional personal data, such as your social media information which typically includes personal details, is likely to violate the principle of data minimization and could infringe upon consent. The game app should work without requiring individuals to provide unnecessary personal data and allow an option to do so at the user's choice.
    Body of Knowledge Domain I, Competency D

36. The correct answer is A. Privacy laws and principles can be complex and full of legal terminology unfamiliar to individuals who do not work in privacy. A data controller needs to balance complexity and comprehensiveness in their privacy notice to ensure that users can properly inform themselves. Otherwise, processing their information is unlawful because consent is invalid. Privacy patterns are real-world, practical design solutions which can be used in in any stage of the development process. Julia is implementing a layered design policy privacy pattern to ensure the user (data subject) is properly informed about her company's privacy practices.
    Body of Knowledge Domain V, Competency B

37. The correct answer is B. The organization would need to apply the least privileged access principle prior to implementing RBAC. This means determining who will need access and which data they need access to. In this way, the company can then appropriately limit access without restricting the employees' ability to do their jobs.
    Body of Knowledge Domain IV, Competency C

38. The correct answer is D. Under the concept of "individual participation," a person should be asked to consent to how their information is being used. Here, where the law is silent (i.e., jurisdictions that do not specifically require consent for collecting and using biometric identifiers), companies can turn to the "individual participation" FIP.
    Body of Knowledge Domain III, Competency A

39. The correct answer is C. Obfuscation prevents ability to read or understand the personal information as presented, but in this case the 'key' or interpretation of the user IDs was not shared with the vendor in order to protect the employees.
    Body of Knowledge Domain IV, Competency A

40. The correct answer is B. People use the same username and password for multiple accounts and subscriptions, making it easier for criminals to use stolen or leaked credentials from one service to access another. Installation and maintenance of IoT devices should employ minimal steps and follow security best practices on usability. Users should also be guided on how to set up their devices securely.
    Body of Knowledge Domain VII, Competency A

41. The correct answer is C. The need for each software update should be clear to users, and an update should be easy to implement. Software updates for IoT devices should be verified before rolling out and an individual should have the option to update or not. If an unauthorized change is detected, the device should alert the administrator of an issue and should not connect to wider networks than those necessary to perform the alerting function. Network segmentation can be applied either as physical or logical segmentation as it helps to contain the spread. There are also some situations where devices cannot be patched. Some ultra-constrained devices will fit in this category. For these devices, a replacement plan needs to be in place and should be clearly communicated to the consumer.
    Body of Knowledge Domain V, Competency B

42. The correct answer is B. Information technology creates or applies solutions for every area of an organization, so adopting a holistic view to the protection and safeguarding of data at all levels of processing will best support a risk management approach to data protection compliance.
    Body of Knowledge Domain I, Competency C

43. The correct answer is B. Beta testing can provide extremely valuable insights – real scenarios of interactions with a product. Privacy concerns during beta testing primarily relate to the scale and openness with which the test is conducted. Unlike alpha testing, user accounts and associated personal data created in beta testing may be retained for the live version of the system. Therefore, changes in privacy policies or other privacy mechanisms for the live system should be introduced to beta users to transition these users to the live system.
    Body of Knowledge Domain V, Competency B

44. The correct answer is C. Considering each group's values and how they may conflict allows for clearer consideration in developing a project and aides in determining an appropriate path forward.
    Body of Knowledge Domain II, Competency A

45. The correct answer is B. Intrusion reporting is about collecting data on how much a software application is used and this enables privacy technologists to detect and better diagnose why the application may not have performed as expected. More importantly, this sort of reporting can enable more robust software designs that are less susceptible to attacks.
    Body of Knowledge Domain III, Competency E

46. The correct answer is A. A record of processing activities (RoPA) requires the listing of operational processes to determine high-risk processing, classification of personal data, and other details such as who has access to the information, where the information is located and when the information is shared. This can be highly useful for all entities as they prepare for audits or investigations from supervisory authorities, manage sensitive data sets and secure data across high-risk activities. A RoPA does not require a collated list of personal data across an entire book of clients, which would likely jeopardize operational efficiency.
    Body of Knowledge Domain I, Competency C

47. The correct answer is C. TLS is a widely used means of encryption. It encrypts data before it is sent to protect the data in-transit and decrypts it upon receipt. Because protection on the receiving end is not a feature of TLS, it is recommended that the sender only share the data with trusted parties.
Body of Knowledge Domain IV, Competency C

48. The correct answer is C. When a part of the business is outsourced, the hiring organization retains accountability. While authority can be delegated, you cannot delegate responsibility. To maintain standards and compliance it is necessary to ensure that the service provider adheres to standards and compliance equally before delegating or outsourcing.
Body of Knowledge Domain II, Competency A

49. The correct answer is A. When deployed widely in public spaces, facial recognition technology can enable large-scale tracking and monitoring of individuals without their knowledge or consent. The capability for nontransparent mass surveillance poses significant risks to personal privacy and civil liberties because it can lead to unauthorized and intrusive surveillance practices that infringe on individuals' right to privacy in public spaces. The other options may be problematic in different contexts, but they do not represent primary privacy concerns associated with facial recognition technology.
Body of Knowledge Domain VII, Competency C

50. The correct answer is A. Blackmail, in a privacy context, relates to threatening to disclose personal data. In this example, a man took what was meant to be confidential information—a female customer's personal data—and used it to attempt to exploit her.
Body of Knowledge Domain III, Competency D

51. The correct answer is D. Increased accessibility is about amplifying the accessibility of personal data. By putting an unmonitored open list at the entrance to the store, the business failed to offer any safeguards for or mitigate the risk to the information they were collecting.
Body of Knowledge Domain III, Competency C

52. The correct answer is C. Data misuse is the use of information in ways it wasn't intended for or wasn't consented to by the data subject. Privacy policies, privacy notices, corporate policies, data privacy laws and industry regulations all set conditions for how data can be collected and used. Data misuse violates these requirements, which could bring about actions at the state and federal levels.
Body of Knowledge Domain III, Competency C

53. The correct answer is D. Phone app users may not be aware they are being tracked despite having provided explicit consent in the past for the phone app to do so. It is important they understand that their personal data is being further collected/shared so that their prior explicit consent remains informed and valid. However, this should be done in an unobtrusive way to prevent what is known as notification fatigue. Privacy patterns are real-world, practical design solutions which can be used in any stage of the development process. In this example, the phone app developer utilized what is known as an ambient notice privacy pattern, which gently reminds the user that their sensitive location data is being shared again.
Body of Knowledge Domain VI, Competency C

54. The correct answer is A. Personal information at rest, in transit and in use must be protected to ensure confidentiality, integrity and availability. Secure Multiparty Computation (MPC) allows two or more computer systems to be used in a computation and compute a mathematical result without otherwise revealing private information that is stored on those systems. For example, payroll is private information that resides within each of the FTSE company. By contributing to the statistical computation without disclosing the actual payroll information through a MPC network, a FTSE company would also benefit from such computations for their own benchmarking purposes.
Body of Knowledge Domain III, Competency D

55. The correct answer is A. Privacy standards must be reviewed and refined on an annual basis at a minimum. To ensure compliance with new laws, the privacy standard needs to be reviewed and refined whenever a relevant new law is enacted.
Body of Knowledge Domain I, Competency C

56. The correct answer is C. Summarizing data establishes categories based on data elements, such as an employee's department, role or location. Summarizing this data is necessary to avoid exposing personal data when information is viewed based on each of these various data points.
Body of Knowledge Domain VII, Competency D

57. The correct answer is C. Privacy engineering involves integrating privacy considerations into product design, which may involve process management and/or technical know-how. Including privacy considerations in the life cycle of software development allows the organization to ensure that privacy measures are evaluated and updated as privacy concerns change.
Body of Knowledge Domain VI, Competency A

58. The correct answer is B. Requests for access should be handled by the privacy team to ensure the requesting party meets the appropriate requirements for access. The request should not be answered by the IT department.
Body of Knowledge Domain II, Competency A

59. The correct answer is B. TristarGlobe Inc. is planning to develop a procedure that will determine what the least amount of personal data needed on the training materials is. That procedure is part of the privacy by design process activity, “identify information needs” covered by EdMed’s “Identify training information needs” SOP. The goal of privacy by design’s “identify information needs” is to determine adequate, relevant and limited personal data for what is necessary to ensure quality training, also known as the data minimization principle.
Body of Knowledge Domain V, Competency A

60. The correct answer is D. Nonfunctional requirements, or quality attributes, define characteristics the system must have, such as “auditability.” Declaring that the system must have the ability to be examined or reviewed will provide all stakeholders with evidence that the data was processed as intended in a transparent manner.
Body of Knowledge Domain V, Competency A

61. The correct answer is B. A PIA (privacy impact assessment) examines how personal data is being processed and what the privacy risks are to that personal data. Knowing where potential risks are allows organizations to address those risks before an incident or breach occurs. Since neither EdMed nor Tristar could provide evidence of a PIA, it is necessary to perform one to ensure that all potential risks are addressed moving forward.
Body of Knowledge Domain I, Competency C

62. The correct answer is C. Supervision enables an organization to enforce privacy policies through processes and demonstrate that other actors, such as TristarGlobe Inc., are compliant with those policies and processes. By documenting findings, it also allows an organization to provide evidence of compliance with regulations, standards or privacy policies to regulators and stakeholders.
Body of Knowledge Domain V, Competency A

63. The correct answer is C. An incident response procedure is the process of documenting the details of the attack, determining the impact and then deciding on the appropriate actions. A privacy audit and IT control review provides a detailed examination of both policy and practice to highlight compliance gaps in the control environment and in IT practices of the organization. A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security. A data protection gap analysis compares the organization’s activities to specific identified compliance requirements and determines where there are gaps that need to be addressed.
Body of Knowledge Domain III, Competency B

64. The correct answer is A. Balance utilizes the strategies of inform and control to reduce imbalances of information and power as David’s company has decided to use legitimate interest as the lawful basis for processing personal data of its customers in the new fraud prevention solution that will benefit the company and its customers. The assessment is necessary to determine that benefits are proportional to any potential risks incurred in terms of legitimacy, appropriateness and adequacy.
Body of Knowledge Domain VI, Competency D

65. The correct answer is B. Interference is a threat to a user's privacy that could potentially lead to harm. This is an example of a decisional interference in which the outcome affects an individual's ability to secure a loan, among other actions.
Body of Knowledge Domain III, Competency E

66. The correct answer is D. A user of a website may assume that when they are not logged in to their profile that their actions are not being associated with or linked to their profile. Cookies that record the IP address and browsing patterns are likely to allow a profile of an unauthenticated user to be matched with a registered profile. This would be surveillance that constitutes a privacy threat since the individual is unlikely to be aware it is happening.
Body of Knowledge Domain III, Competency B

67. The correct answer is B. Privacy engineering's goal is to ensure that privacy-protective solutions are developed in line with business need. The others are incorrect as data security considerations are a part of privacy engineering considerations; anonymization is not a mandatory requirement for all personal data; and legal basis of processing considerations is not a primary consideration of privacy engineering goals.
Body of Knowledge Domain VI, Competency B

68. The correct answer is C. We do not know enough about the data set to determine an appropriate value for k-anonymity. Because there is the potential for reidentification and the dataset contains potentially sensitive information, the dataset should be properly anonymized prior to being sold.
Body of Knowledge Domain IV, Competency C

69. The correct answer is B. Closed-source software can only be fixed by the vendor, as the underlying code is proprietary, and consumers may need to wait to be assisted with issues. This could create problems for the retailer if it needs to act immediately to resolve a threat or address possible risk factors.
Body of Knowledge Domain III, Competency E

70. The correct answer is B. In practice, privacy professionals often have restricted resources and performing a proactive review of all assets regardless of whether there have been changes or not is not an effective use of those resources. Setting up an alert system may sound like a solution to the problem of non-specific monitoring, but in practice if the SME is alerted for every single change generally what happens is that the individual receives so many email alerts that they stop reviewing them and may even filter them to a folder. Finally, the data protection audit is not an effective monitoring tool because it happens too infrequently and is measuring against a point in time that has since been superseded so this is also an ineffective form of monitoring. The best practice is to train all staff to follow standard operating procedures so that they inform the privacy compliance subject matter expert of any significant changes. This allows the SME to be discerning and targeted, while staying on top of anything relevant so they are up to date.
Body of Knowledge Domain VI, Competency D

71. The correct answer is C. The respect for user privacy principle supports the building of trust by having data subjects play an active role in the management of their data. The privacy by design principle of respect for user privacy is also supported by several Fair Information Practice Principles (FIPPs), including consent.
Body of Knowledge Domain I, Competency A

72. The correct answer is C. Bug reports contain various types of information, including software version, crash description, reproducing steps, reproducing test cases, etc. including user details. It is the responsibility of the application team to develop mechanisms to encrypt data in transit and storage while performing bug tracking and reporting.
Body of Knowledge Domain III, Competency B

73. The correct answer is A. Ann Cavoukian's Privacy by Design framework, Principle 1 (Proactive not Reactive; Preventative not Remedial) calls for preventing privacy harms before they happen. One of the best ways to do this is through data minimization and removing personal data wherever possible. The data has been de-identified and aggregated as the stated secondary purpose is to assess facilities utilization making it unnecessary to know "who" has been in the office, just that there has been a person there. Statistical, non-personal data is all that is needed to achieve the new purpose for the data. Principle 4 (Full Functionality – Positive-Sum, not Zero-sum) is also relevant in designing a "win-win" solution where privacy can be respected (risk mitigated) and data can be repurposed to achieve additional, legitimate business objectives.
Body of Knowledge Domain I, Competency B

74. The correct answer is C. Employee monitoring is complicated. Certainly, there is a legitimate interest in ensuring your employees are productive, but employment and privacy laws require that the employer and employee interests are appropriately balanced. An organization should consult with its legal department or representatives to confirm monitoring practices are legally compliant.
Body of Knowledge Domain VII, Competency D

75. The correct answer is C. Summarizing detailed information into categories based on more abstract attributes and restricting access to summary information is the correct answer. It describes the abstract (summarize) and hide (restrict) strategies for securing data domains.
Body of Knowledge Domain VI, Competency D

76. The correct answer is A. Subject to any legal requirements, companies can effectively mitigate privacy, security and regulatory risks by removing unneeded personal data from their systems. Anonymization is another step that can be taken, although not provided in these options. Many privacy regulations, such as the GDPR, CCPA and HIPAA, require a thorough analysis to determine whether data has been sufficiently anonymized and no longer identifies an individual. Companies should consider statutory and regulatory guidance when deleting or anonymizing data. They should also consider how the information they collect or retain could be combined with publicly available information to reidentify the data.
Body of Knowledge Domain IV, Competency A

77. The correct answer is B. The other actions are options better designed to eliminate bias. Inputs are important when it comes to automated decision-making as often input contain biases and discriminatory patterns. Even if great care is taken with inputs, outcomes should still be monitored and reviewed to minimize bias/discrimination. Additionally, a regular review of the tool to ensure it is generating fair outcomes, as well as having humans oversee the tool are all ways to minimize bias and discrimination.
Body of Knowledge Domain III, Competency A

78. The correct answer is A. The area specialist bridges the technical gap between software engineering and privacy and consults across multiple IT projects within an organization to share privacy knowledge. Area specialists also collect critical regulatory requirements from lawyers; validate that marketing requirements are consistent with laws and social norms; meet with designers to discuss best practices when translating requirements into design specifications; collect user feedback and monitor privacy blogs, mailing lists and newspapers for new privacy incidents. Project managers ensure that adequate resources are available to construct the system and that team members communicate effectively during construction, deployment and maintenance. Programmers translate software design into source code using best practices and standard libraries and frameworks. Administrators install and maintain the software.
Body of Knowledge Domain II, Competency A

79. The correct answer is B. In privacy, a traceability matrix also connects requirements to user agreements, such as privacy policies, terms of use (ToU) agreements, end-user license agreements (EULA) and so on. When conducting a traceability exercise or whenever a requirement or IT system component changes, the trace matrices should be consulted to determine the impact of the change on other parts of the system, including privacy policies.
The correct answer is Domain IV, Competency B

80. The correct answer is C. Information asymmetry is generally described as one party (the research organization) having more or better information about a transaction than the other (Linda). The registration should require minimal information from Linda, so that only as much personal data as is required, explained and consented to, is processed. Further reduce the imbalance of policy knowledge by providing clear and concise policies (written and verbal in some cases) rather than, or in addition to, complex and verbose ones.
Body of Knowledge Domain VI, Competency C

81. The correct answer is B. The concepts of privacy threats and violations during data collection is focused on instances where data is being collected from the individual for whom it pertains. An interviewer asking a candidate an inappropriate question (e.g., about their sexual orientation or marital status) when this has no bearing on the candidate's ability to do the job is likely a violation of the candidate's privacy. Additionally, collecting this type of personal data may result in a violation of regional laws or claims of discrimination.
Body of Knowledge Domain III, Competency B

82. The correct answer is B. Specific requirements vary by jurisdiction, but current customers should be given notice of any changes in how their information is being used or who may be accessing it. When using an API, personal data may be exposed or logged through remote call procedures, and often technical explanations are insufficient for customers to fully understand the implications of new features or technologies.
Body of Knowledge Domain IV, Competency B

83. The correct answer is B. Data encryption uses algorithms to encode data into an unreadable format that needs an authorized key for decryption. It is recognized as one of the most reliable ways to keep data confidential at rest, in-transit, or when processing real-time analytics.
Body of Knowledge Domain IV, Competency C

84. The correct answer is A. A merger or acquisition can introduce differences in data processing practices, differing approaches to privacy risk management and operational aspects that are inconsistent or even incompatible with the other. The rest of the options do not align with commonly known PIA triggers.
Body of Knowledge Domain II, Competency B

85. The correct answer is C. More web browsers, including Safari and Firefox, now block third-party cookies by default. Technologies that rely on third-party cookies will need to adjust their practices to account for browsers that come with built-in privacy protections. In this case, FraudNoMore is marking all transactions as fraud when their third-party cookies are unable to be collected. As more browsers disable this type of tracking by default, requiring third-party data collection and tracking to make a purchase is both an anti-privacy and anti-business approach. There are first-party mechanisms available to allow this type of fraud detection within privacy frameworks such as Apple's Intelligent Tracking Prevention (ITP).
Body of Knowledge Domain VII, Competency B

86. The correct answer is D. Device fingerprinting is the technique used to create a unique picture of a given user based on a series of datapoints. Many of these data points on their own are harmless, but together, are unique enough to create a very high probability that if another device with the same characteristics is seen again, it is the same individual as before. The data collected in this case includes cookie IDs in addition to IP address, device operating system, device type, browser name, screen size, browser language and list of browser plugins installed.
Body of Knowledge Domain VII, Competency B

87. The correct answer is A. Email open tracking is done via use of a tracking pixel or other images or code within the body of an email. When you open an email, the tracking pixel is loaded, and the organization receives a signal that a specific email address has opened that email. Many email clients now block images by default. When images are blocked by default, the tracking pixel is not loaded when the email is opened. If the pixel is not loaded the company does not receive a notification that the email was opened.
Body of Knowledge Domain VII, Competency B

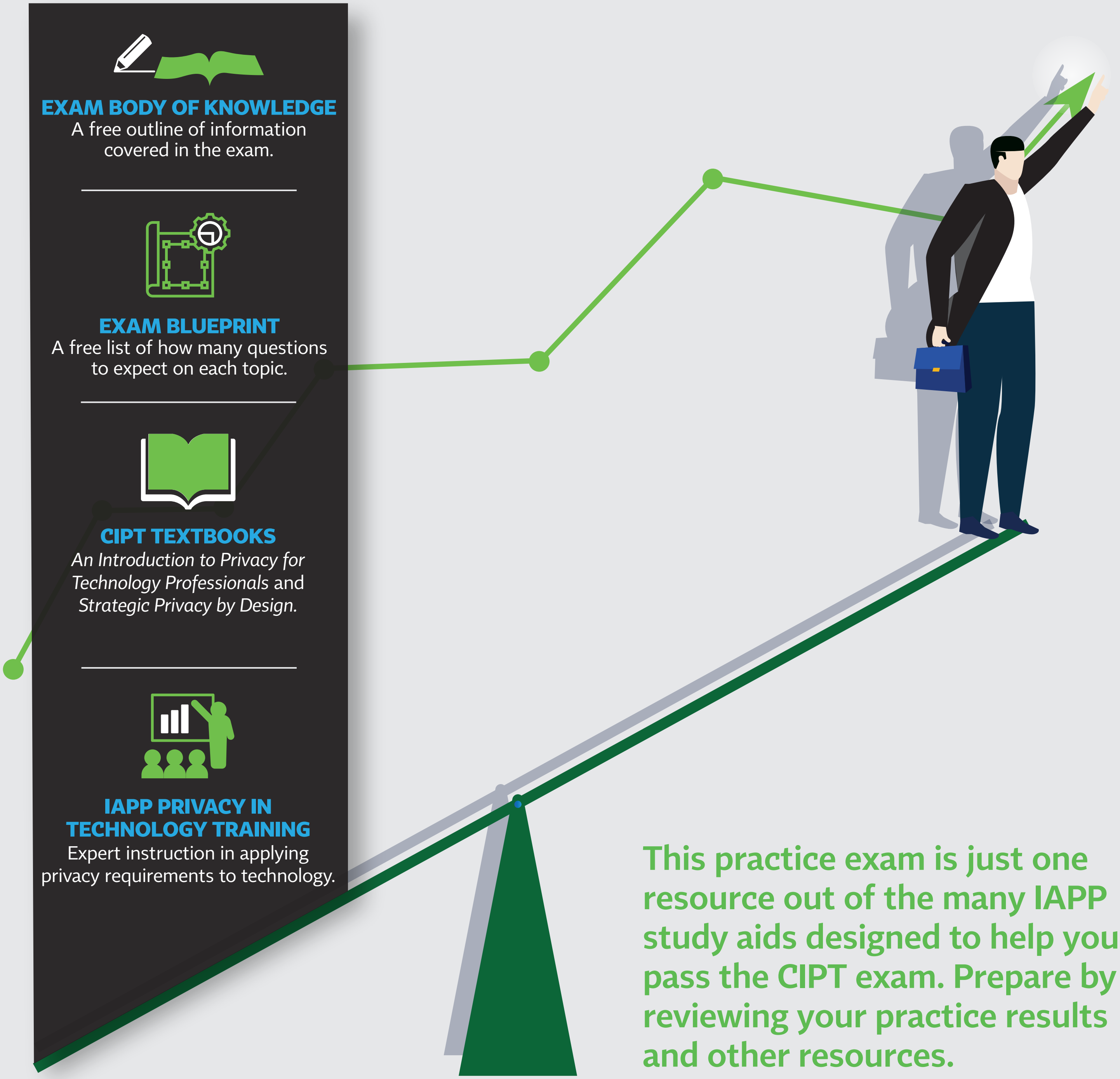
88. The correct answer is B. Many web browsers allow website operators to request location data from end users. When this location consent is granted, the web browser will use a variety of signals to determine the most precise location. The signals used depend on the device, but generally it will rely on the most accurate technology available on that device. For example, if location is granted on a cell phone, the browser is able to leverage very precise geo-location based on the GPS data from the cell phone. However, even if the user declines to share their location with the website, their IP address is always sent to a web server as part of normal network communications. Many websites leverage this information to tailor the website to you, regardless of your browser-level location settings. As privacy is becoming more mainstream, website operators are considering to what extent IP addresses should be used without permission for purposes other than its necessary usage in delivering the webpage.
Body of Knowledge Domain VII, Subdomain B

89. The correct answer is D. Each of the items listed must be considered when choosing to deploy an app. However, reviewing the agreement for compliance with your own policies is the final consideration listed here. Ensuring your company understands fully how the use of the app will affect your customers/the users must be done before signing any agreements with the developer.
Body of Knowledge Domain III, Competency B

90. The correct answer is C. Allowing customers to access and correct their personal data through a secure online portal ensures that the supermarket chain supports individuals' privacy rights requests effectively. This reflects the importance of providing customers with control over their personal data, aligning with the principles of transparency and user empowerment.
Body of Knowledge Domain II, Competency B

iapp

Build on Your Practice Exam Results



EXAM BODY OF KNOWLEDGE
A free outline of information covered in the exam.

EXAM BLUEPRINT
A free list of how many questions to expect on each topic.

CIPT TEXTBOOKS
An Introduction to Privacy for Technology Professionals and *Strategic Privacy by Design.*

IAPP PRIVACY IN TECHNOLOGY TRAINING
Expert instruction in applying privacy requirements to technology.

This practice exam is just one resource out of the many IAPP study aids designed to help you pass the CIPT exam. Prepare by reviewing your practice results and other resources.

Certified Information Privacy Technologist
CIPT
iapp

Go to **iapp.org/train** to find these and other resources that will help you feel confident and prepared for your CIPT exam.