CIPM PRACTICE EXAM

An iapp publication

CIPM® Practice Exam

An IAPP Publication

v1.1

About the IAPP CIPM Practice Exam

The IAPP CIPM practice exam is designed to support your preparation for the CIPM certification exam. Developed using IAPP study resources as well as subject matter experts' practical knowledge of the topics set forth in the IAPP's CIPM body of knowledge (version 4.1.0), the practice exam can help identify your relative strengths and weaknesses in the major domains of the CIPM body of knowledge. It was developed to simulate the types and breadth of questions you may encounter on the CIPM 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 CIPM practice exam were reviewed for accuracy at the time of publication.

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

Do you have questions or comments?
Please contact us at training@iapp.org

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 three-page 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 sub-domain 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 Ⓐ Ⓑ Ⓒ Ⓓ

CIPM Practice Exam

1. What is the purpose for undertaking a privacy maturity assessment?

   A. A maturity assessment assists an organization with determining the age demographics of the employees within the businesses that they operate.
   B. The maturity assessment is a metric that enables an organization to assess and compare privacy practice deficiencies between its workforce teams.
   C. The maturity assessment enables an organization to evaluate the privacy practices of the business and determine how best to prioritize the actions needed to improve.
   D. The maturity assessment enables read access logging to set a benchmark to identify the success or failure of improvements made to privacy programs and processes.

2. Under the privacy maturity model (PMM), what must an organization include in its privacy program to move from a maturity level of "defined" to a maturity level of "managed"?

   A. Document and report all processes and procedures.
   B. Establish and authorize a privacy management team.
   C. Measure and control processes to establish effectiveness.
   D. Determine and comply with applicable legal requirements.

3. Which of the following is an employee privacy concern that can be addressed through an HR policy?

   A. Employees' access to offered benefits.
   B. Employees' professional development courses.
   C. Employees' compliance with accrued time-off policies.
   D. Employees' personal communications on work devices.

4. A company's data center suffers a short power outage and the backup generator does not kick in. After services are restored, some of the personal data processed by the company appears to be lost. What should the privacy team do first?

   A. Consult with the incident response team.
   B. Notify appropriate regulatory authorities.
   C. Determine which data subjects are affected.
   D. Disclose the potential incident to all data subjects.

5. When measuring privacy, which component of analysis concentrates on the reporting data that remains when the other components of the series, primarily time and cyclical, have been accounted for?

   A. The trending component.
   B. The irregular component.
   C. The automated component.
   D. The operational component.

SCENARIO I

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

You have recently been hired on as privacy officer for a newly-formed, privately-funded kidney dialysis company based in Boston, Massachusetts in the U.S., with subsidiaries in Dublin, Ireland and Dubai, UAE. The company's focus is on utilizing artificial intelligence software to manage and enhance care for end-stage kidney disease patients around the world by analyzing patient data and making predictions that allow "right care at the right time". Most of the company's employees will be located within close proximity to the three main offices; however, the sales team, which makes up approximately one-third of the workforce, will have the ability to work remotely full-time since much of their work will be spent travelling to customer locations to demonstrate and train on the new software. While headquartered in the U.S., the company delegates broad decision-making authority to its two subsidiaries, allowing the subsidiaries to have control of their day-to-day business functions. As part of this delegation of control, the privacy team has privacy professionals in each region to support privacy within its subsidiaries. The company has chosen to outsource its information security functions utilizing a third-party vendor. All customer data will be stored in a cloud-based server. Access will be restricted in a manner that only allows each subsidiary to view and access customer data for their own country's customers. For example, employees based out of Boston will not be able to access the customer data for Dubai's clients. Certain leadership employees will be able to see across all three locations; however, their access will mainly be to non-customer-specific data.

You have a strong background in managing privacy programs in U.S. healthcare organizations. Previously, however, you have only worked at not-for-profit U.S. organizations; this will be your first time working at a for-profit global company. You will be reporting to the chief compliance officer (CCO), headquartered in Boston, who has expertise in the operations of a global kidney dialysis company and general knowledge regarding compliance regulations and laws to which the new organization will be subject. While the CCO has some knowledge of privacy laws and regulations that may impact your new organization, she will be relying on you to ensure company compliance from a privacy program management perspective. Both you and your boss' roles will entail ensuring all subsidiaries comply with all country-specific laws, regulations and norms. You are well aware of the importance of buy-in at all levels of the leadership in order for the privacy program to be effective and are eager to show your new boss how you can apply that knowledge and expertise to ensure the company is appropriately addressing all privacy risks facing the organization.

6. You have been asked to develop a mission statement and code of conduct for the company's privacy program that will be reviewed and approved by executive leadership. What should your primary focus be when developing these two foundational documents?

   A. Referencing all laws and regulations that may impact the company from a global perspective.
   B. Ensuring alignment with corporate business objectives across the company to include the subsidiaries.
   C. Determining how the organization will enable future expansions to allow necessary access to appropriate data.
   D. Making certain that it is reviewed and approved by primary regulators in all three countries where the company has offices.

7. Which of the following methods would be the most efficient and effective method for administering a privacy training program to your company's workforce?

   A. Develop and administer privacy training for all employees reflecting the needs of all locations.
   B. Develop and administer privacy training that focuses solely on overarching privacy guidelines.
   C. Develop and administer privacy training that aligns with employees' roles regardless of location.
   D. Develop and administer privacy training for each location incorporating overarching requirements.

   END SCENARIO I QUESTIONS

8. Considering that a data incident is typically viewed as a "when, not if" situation, organizations need to have an incident response plan in place. Which of the following lists two of the five categories of incident preparedness?

   A. Understanding key stakeholders and managing vendors.
   B. Auditing privacy policies and reviewing industry standards.
   C. Consulting with the regulatory authority and reviewing risk factors.
   D. Training employees and engaging the IT team for data processing review.

9. If a data controller outsources activities pertaining to personal data management then accountability for compliance is retained by the controller. Which type of audit would be appropriate for this situation?

   A. A supplier audit.
   B. An internal audit.
   C. A standardized audit.
   D. An independent audit.

10. A prospective vendor should be evaluated against standards through questionnaires, privacy impact assessments and other checklists. An initial standard for selecting vendors should include which of the following?

    A. Vendor Location.
    B. Contract analysis.
    C. Industry Reputation.
    D. Termination procedures.

11. To collect and process personal data, a particular healthcare provider is required by law to obtain explicit consent from its patients. A privacy notice is published on the provider's website informing the patients of how their data will be processed. Before giving their consent, the patients must acknowledge that they read and understood the notice. What process should the healthcare provider have in place to avoid misunderstanding and reduce the risk of potential legal claims?

    A. Sending each consent along with the privacy notice to the data protection officer.
    B. Recording the date and time of consent in the appendix of the internal privacy policy.
    C. Publishing patients' consents on the website as testimonials to attract new customers.
    D. Storing the privacy notice provided to the patients along with the record of their consent.

12. Which of the following best defines data governance with respect to personal data?

    A. A privacy framework that defines the processes and procedures for how organizations approach the entire data life cycle.
    B. A government directive on the need to define the mission, vision and values of the organization regarding data processing.
    C. An organizational roadmap detailing five years' worth of key performance indicators on achieving data processing objectives.
    D. A chart showing the roles of the employees in the organization and their essential responsibilities regarding data processing.

13. Which of the following is one way that global organizations ensure that proposed privacy policies align to local laws?

    A. Establish a governance structure consisting of representatives from various geographic regions.
    B. Complete privacy impact assessments (PIAs) and implement privacy by design and default for all new products.
    C. Create an internal audit team to complete their own review of the organization's current privacy program.
    D. Drive future business using "good data protection" principles set forth by the business development and strategy department.

14. Betty, a member of the privacy team, has been asked to consider the effectiveness of her company's privacy framework. To do so, she has been conducting interviews with employees across the business, from senior executives to the customer service staff. Betty has found that, in general, back-office employees are aware that there are documented privacy policies and procedures in place, but they are not able to confidently explain what they say nor how personal data is handled by the company. Betty has also found that, in general, employees who have direct interaction with customers have a clear understanding of what personal data is, but they are less familiar with documented procedures or what compliance obligations the company has. Of the following options, which is the best suggestion Betty can make to the company?

    A. The company should continually monitor, maintain and improve the maturity of its privacy program and ensure that privacy managers maintain personal data properly.
    B. The company should prepare a report so there is a formal record of the findings, including facts, evidence, best practices and standards to help assess the current situation.
    C. The company should improve its privacy training program to ensure all employees have accountability and are aware of the company's documented procedures and legal obligations.
    D. The company should not change anything as its framework is operating effectively. Employees at various levels know the basics of what they need to know about privacy and personal data.

15. Which of the following is an example of a technical control used to safeguard personal data during the privacy operational life cycle?

    A. Obfuscation.
    B. Security training.
    C. Data classification.
    D. Data protection policy.

SCENARIO II

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

Mollie has been a customer of a popular online retailer for a women's fashion brand for over 10 years. Mollie is a frequent shopper and a "VIP customer." As such, she often gets early access to sales and special offers and had a dedicated account manager, Toby. Mollie often communicated with Toby via phone, email and text about order updates, special offers or even complaints. Toby was always on hand to resolve issues and has provided excellent customer service for Mollie. Over the last year, Mollie has noticed she has had to return several items for a variety of reasons. Mollie also recently moved and has repeatedly asked for her address details to be changed on her account; however, her deliveries are still going to her old address, causing unnecessary delays. A few of the purchases Mollie returned have not been refunded to her. She even agreed to receive the refunds in the form of gift vouchers or credit applied to her account, but those have not been applied. Her account manager has been replaced by Karen, who is not as easy to contact as Toby, and who often doesn't respond to her messages.

Mollie received a notice that her account information may have been compromised by a data breach, which the company is currently investigating. No further details about the breach have been provided to Mollie. She is becoming increasingly worried and disappointed by the lack of customer service and information provided on the data breach, considering she has been a loyal customer for many years. Because of this, Mollie has not been purchasing as many items and is worried she may lose her "VIP" customer status. Additionally, she is still owed money from many returns that have not been processed and has concerns about identity theft. Mollie reaches out to the generic customer service team rather than Karen. She is escalated to the complaints team, who have already been investigating her complaints for the past month. Despite several attempts to reach the complaints team, she isn't getting any updates. Mollie decides to hire an attorney to take legal action on her behalf.

16. After consulting with her attorney, Mollie allows them to create a data subject access request (DSAR) on her behalf. How should the fashion retailer respond to the attorney?

    A. Confirm in writing with Mollie that the legal representatives have the authority to act on her behalf.
    B. Verify whether the legal representative is actually from a reputable law firm or legal consultancy.
    C. Withhold the information from the legal representatives, as they are not entitled to the information.
    D. Only supply the information to Mollie directly rather than corresponding with the legal representatives.

17. Which of the following information would <u>NOT</u> be provided to Mollie under a data subject access request?

    A. The order history of all purchases Mollie made.
    B. The exact information compromised in the data breach.
    C. The conversations Mollie had with account representatives.
    D. The process through which her account manager is selected.

END SCENARIO II QUESTIONS

18. When assessing how privacy practices are managed within an organization, what is the role of the ethics and compliance department?

    A. Develops and defines data protection risks which are included in the organization's enterprise risk management framework.
    B. Responds to any complaints or whistleblowing incidents relating to how an individual's personal data may have been handled.
    C. Reviews and ensures that the appropriate data privacy contractual language is in place with any contract between the organization and a third-party service provider.
    D. Determines whether the proper controls are in place to protect personal data and ensures that each of these controls are being followed by the people within the organization.

19. You are looking to write a data classification policy for the entire organization. One issue is that each department has different types of data and other requirements for that data. How should you manage this policy and its rollout?

    A. Write the policy and send it to department heads to socialize amongst their employees with the provided training.
    B. Write the policy and ensure that employees attest that they have read and understand it and will comply with it, then monitor compliance with audits.
    C. Write the policy, and then write standard operating procedures containing standard minimum controls for each department, with feedback from data owners.
    D. Write standard operating procedures (SOPs) for the entire organization to support the policy and tie compliance to the SOPs and policy to performance goals.

20. Under which of the following circumstances is a data protection impact assessment (DPIA) required in the EU?

    A. When using automated decision-making with significant effects.
    B. When an organization regularly collects the data of well-known individuals.
    C. When personal data is being processed by companies with multiple locations.
    D. When an organization and its affiliates combine the data of existing data subjects.

21. Which of the following contains information about whether a company discloses personal data to third parties?

    A. An internal audit.
    B. A data inventory.
    C. A security incident plan.
    D. A privacy impact assessment.

22. Before entering into any new business relationships or renewing old contracts with vendors, what should an organization do as a key component of securing the service?

A. Create a third-party processor and vendor checklist.
B. Carry out a third-party processor and vendor assessment.
C. Classify the vendor or processor according to their system access.
D. Review service-level agreements (SLAs) to assure parties perform as expected.

SCENARIO III

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

GoodGifts.com is a gift company that provides businesses with the ability to order a variety of physical gifts to send to their employees. The business is completely web-based, and the website for ordering is hosted by a third-party software company. All products are sent via a national shipping company. GoodGifts.com is careful to maintain separate databases for each client along with appropriate firewalls and security measures.

Businesses have the option to select specific gifts for each employee, or GoodGifts.com can select the items for the business based on the age of the employee. General guidelines for gifts can be provided to select or omit specific items, such as gift cards, humorous items or alcohol, allowing businesses to adjust their employee gifts to align with the company values and culture.

A national supermarket chain in the U.S. has a contract with GoodGifts.com to send an age-appropriate birthday gift to nearly all of its 7,000 employees on their birthdays. The supermarket's point of contact provides GoodGifts.com with each employee's name, address and birthdate, including birth year, and the gift items they wish to have included as options. All employee data provided by the supermarket is encrypted.

During a routine audit, an administrator at GoodGifts.com identified a potential data breach. Upon further investigation, they concluded that there was a breach of their systems wherein the personal data of 553 of the supermarket's employees was compromised. None of GoodGifts.com's other clients' data was affected. GoodGifts.com notified the appropriate supervisory authorities and those individuals whose information they identified as having been directly affected by the breach.

23. Who else should GoodGifts.com notify about the data breach?

A. Third-party web host, the supermarket's point of contact, the remaining supermarket employees.
B. Shipping company's privacy department, all of GoodGifts.com's other customers, local law enforcement.
C. Third-party web host's other customers, GoodGifts.com's employees, state attorney general's office.
D. All individuals in each of GoodGifts.com's client databases, third-party web host, shipping company employees.

24. GoodGifts.com was able to manage the breach with relatively minor impact to personal data and therefore to individuals. Which of the following was NOT a contributing factor to minimizing the impact?

    A. Regular audits.
    B. Client contracts.
    C. Data encryption.
    D. Separate databases.

25. Why is it important to review privacy impact assessments on a regular basis?

    A. Because customers' privacy expectations can change frequently.
    B. Because it ensures employees are complying with privacy practices.
    C. Because technology can change throughout the lifecycle of a product.
    D. Because it is evidence of the company's commitment to good privacy practices.

    END SCENARIO III QUESTIONS

26. Which of the following is a reason for having an executive sponsor for the organizational vision for privacy?

    A. An executive sponsor is the internal subject matter expert and employee liaison.
    B. An executive sponsor ensures the privacy vision is well aligned with the company strategy.
    C. An executive sponsor monitors the expenditure versus the budget for the privacy program.
    D. An executive sponsor liaises with the supervisory authorities on privacy incidents and notices.

27. A local dentistry business, Dr. John & Associates, intends to convert paper-based records on clients to an electronic format to adopt online booking and payment systems for clients. When would it be recommended the business conducts a privacy threshold analysis?

    A. Annually, to identify, test and highlight vulnerabilities in the security posture at various stages of data processing.
    B. During the root cause analysis of the clinic's first data breach to identify the vulnerabilities found during information exchange.
    C. Prior to the privacy impact assessment to determine what data processing will occur and the risks associated with that processing.
    D. During the privacy impact assessment to determine the level at which the business can mitigate the risks associated with the exchange of information.

28. Based on budget and time constraints, which of the following is the best approach for a company to take when identifying legal requirements as part of a privacy program framework?

A. Companies should focus only on the most relevant regulations and the strictest requirements for their primary jurisdictions.
B. Companies need to ensure they comply with different privacy regulations around the world, regardless of the company's location.
C. A company should keep up with the latest changes in privacy laws around the world and adjust policies to meet those legal requirements.
D. Companies should approach legal compliance based on their location and whether they operate in multiple jurisdictions administering privacy laws.

29. Which of the following outlines the standard phases for an audit life cycle?

A. Planning, audit, reporting, preparation, follow up.
B. Planning, preparation, audit, reporting, follow up.
C. Reporting, planning, audit, preparation, follow up.
D. Preparation, planning, audit, follow Up, reporting.

SCENARIO IV

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

A colleague in the Human Resources (HR) team wants to send out a survey to all employees to give feedback on how well their company is supporting the wellbeing of its employees. This will help them look at what they are doing well and what they need to improve. The colleague wants to use a third-party platform to collect and analyse the data to share with the line managers of their direct reports to discuss with them.

30. Which of the following are best practice for access control procedures?

A. Providing access to all the data to all line managers so they can compare notes across teams.
B. Allowing HR to decide who should have access to the platform based on the organizational need.
C. Ensuring the entire HR team has access to all the data to allow them to discuss overarching issues.
D. Giving the data privacy team access to all the data to carry out a Data Protection Impact Assessment.

31. The third-party platform has completed the vendor due diligence required. Which of the following would indicate the most critical risk?

A. The high volume of employees.
B. The data being automatically analyzed.
C. Line managers having access to the platform.
D. The responses of individual employees available in the platform.

END SCENARIO IV QUESTIONS

32. A small IT company offers customer relationship management (CRM) software to other businesses across five continents but is facing serious budget constraints. The company has appointed its first data protection officer (DPO) to implement a privacy program. To help ensure the success of the program, what should the DPO do first?

A. Set up the various required operational and technical measures to respond to all regulatory requirements.
B. Implement a centralized governance model to place planning and decision making under the DPO's control.
C. Ensure external audits are carried out to mitigate risks of regulatory sanctions that would harm company finances.
D. Obtain executive assurance to support the privacy program, including, but not limited to, financial resources.

SCENARIO V

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

A Europe-based snacking company, GoodSnack, has been driving expansion through acquisition for the last few years. As part of its expansion, it has acquired several new businesses, including:

- HealthySnack, which offers a range of healthy snack products that are mainly sold in Europe, but has a growing customer base in Canada, Australia and New Zealand.
- PharmaSnack, the snacking division of a global pharmaceuticals giant. PharmaSnack sells a wide range of medicated products through its direct-to-consumer online portal.
- SnackAI, an India-based startup that uses artificial intelligence to predict consumer snacking behavior.

Just after it acquires HealthySnack, GoodSnack learns of a data breach that occurred in HealthySnack's Australian division, which exposed personal data from its Australia/New Zealand customer base. The breach was traced to a third-party website where consumers were encouraged to register and post pictures of themselves with HealthySnack products. The images were then visible on HealthySnack's social media channels. The investigation by the Office of the Privacy Commissioner of New Zealand found that while the breach was attributed to a zero-day exploit, HealthySnack had failed to assess risks of the processing of consumer data by a third party.

Following a wider review by parent company GoodSnack, an internal audit has found HealthySnack to be deficient in its privacy practices—especially privacy risk assessments—and seeks to ensure all its subsidiaries have adequate privacy measures in place. You have been recruited by GoodSnack and tasked by the audit board with designing and implementing a global privacy assessment process, as well as with assessing any solutions already in use.

From your data gathering, it is clear that SnackAI's expertise can support GoodSnack's strategy to use artificial intelligence to target its marketing activity. Any privacy risk assessment developed for GoodSnack will need to assess the impact of AI. GoodSnack is creating a central data repository of all customer data from GoodSnack and its subsidiary companies to look for direct marketing opportunities. GoodSnack also intends to share data with SnackAI to develop a customer-specific pricing and discount model based on previous purchase history.

33. When conducting a privacy impact assessment (PIA) of SnackAI's additional processing of the combined marketing dataset to develop a customer pricing and discount model, what is the additional privacy risk?

    A. Security. When moving and combining the data, the security controls will need to be enhanced to address the risk of a combined dataset.
    B. Compliance. The additional processing will make it difficult to ensure that SnackAI is in compliance with the regulations to which it is subject.
    C. Healthcare. PharmaSnack's sale of medicated products increases the risk that SnackAI could potentially be processing healthcare data without realizing it.
    D. Legitimate processing. When moving customer data from SnackAI, the original privacy notices should be reviewed to see if they allow data to be shared with the wider group.

34. Which of the following factors of GoodSnack's new global privacy threshold assessment is most likely to trigger the requirement of a DPIA under the GDPR?

    A. Collecting financial data.
    B. Expanding market reach.
    C. Creating marketing profiles.
    D. Expanding product availability.

35. You have completed the design of your PIA/DPIA process, including supporting documents, and are ready to roll them out. As a final step, you are asked to consider when it would be appropriate to update and reapprove each PIA/DPIA. Which of the following statements most accurately answers that question?

    A. PIAs/DPIAs remain valid for the lifespan of the processing activity.
    B. PIAs/DPIAs should be reviewed for updates after a fixed three-year period.
    C. PIAs/DPIAs should be reviewed following any security breach investigations.
    D. PIAs/DPIAs should be reviewed based on the risk level of the processing activity.

    END SCENARIO V QUESTIONS

36. Of the following options, which is the best way for an organization to handle communication of a personal data breach?

    A. The company should inform employees properly so that they know how to handle questions from customers.
    B. The company should keep the breach completely confidential to avoid the risk of reputational harm to the company.
    C. The company should keep the breach confidential and only notify authorities once all the details have been reviewed.
    D. The company should make the breach public to ensure the company is held accountable for the way it handles personal data.

37. It is important to consider which of the following when determining the scope of a privacy program?

A. The advantages of a decentralized governance model.
B. The structure, roles and responsibilities of the privacy team.
C. The personal data collected and processed by the organization.
D. The conditions for appointing a DPO listed under Article 37 of the GDPR.

38. Company X, based in Europe, is acquiring Company Z, which operates in Europe as well as other regions. As part of a plan to integrate Company Z's employees into its systems, Company X is about to run some test loads of employee data to ensure completeness and accuracy. To appropriately address privacy concerns under the GDPR, what should Company X do first?

A. Send its employee data protection notice to Company Z's employees prior to any processing.
B. Cancel any scheduled data transfers, as testing on live data is not allowed in the EU under the GDPR.
C. Transfer the employee data to start the test loads and ensure accuracy—an important privacy principal.
D. Company X should not need to take any additional steps since it already operates within the jurisdiction of the GDPR.

39. There was a recent theft at your office building where your organization rents a suite. Management would like to provide the board of directors with the assurance that the suite is secure by conducting an audit of the physical safeguards. Select the response that will solely audit the physical safeguards on premises?

A. Clean desk policy, non-disclosure agreements, background checks, locked cabinets.
B. Background checks, employee privacy policy, privacy breach reporting, complaints log.
C. HR eLearning records, non-disclosure agreements, privacy consents, public-facing website.
D. Clean desk policy, locked cabinets, access-controlled entry, power down of office computers.

40. A privacy team should work with information security and IT to ensure effective access controls. Which of the following is a basic security principle for role-based access controls (RBAC)?

A. Least privilege. Grant access at the lowest possible level required perform the necessary function.
B. Classify. Information privacy classifies personal data into two categories: personal and sensitive.
C. Rank and prioritize. Not all problems can be solved or mitigated at once and ranking is key for resource allocation.
D. Allocate resources. Increased involvement of privacy personnel on information security teams and vice versa.

41. Which of the following is necessary to ensure an organization has an efficient and consistent process for handling data subject complaints?

A. Employees must understand how to authenticate data subjects.
B. Employees must understand the legal impact of noncompliance.
C. Employees must understand the types of requests the organization may receive.
D. Employees must understand the technical processes for complying with requests.

42. What is considered to be the main benefit and objective for having a privacy program framework?

    A. It helps a business maintain privacy and data governance and prevent data breaches while complying with regulations.
    B. It helps a business understand the key drivers behind privacy in an operational context and assign ownership to privacy champions.
    C. It enables a business to evaluate and improve the efficiency of its privacy compliance processes while advancing its business goals.
    D. It ensures the correct compliance policies and procedures are in place while providing flexibility to adapt practices to suit commercial requirements.

43. A new online retailer has emerged as the result of the amalgamation of several international retailers. They have hired you as a privacy consultant to support their global marketing strategy. The new retail company collects and uses personal data for the purpose of email marketing communications to individuals. What do you recommend to the retail company as the best way to screen the organization's use of personal email addresses?

    A. Review and update the published privacy notice on your public-facing website to notify individuals.
    B. Monitor the systems and processes associated with obtaining and withdrawing privacy consent regularly.
    C. Mail a copy of your marketing materials to the individual's home address annually as a form of notification.
    D. Provide ongoing training to your customer service agents on your organization's marketing and privacy practices.

44. An organization signs an agreement with a new vendor who, on behalf of the organization, will process the personal data of the organization's customers. What personal data processing best practice should the organization follow after engaging with this new vendor?

    A. Update the data processing inventory.
    B. Assess the vendor's privacy risk threshold.
    C. Send the vendor agreement to all customers.
    D. Inform regulators of your relationship with the new vendor.

45. Your organization recently suffered a breach of security safeguards where personal information was lost due to a sophisticated phishing scam that targeted employee personal information. There are significant expenses attributed to the breach. The Senior Privacy Director has requested that you review and recommend changes for the budget allocated to privacy breaches. What would you do to get leadership buy-in for the increase in budget allocation?

    A. Conduct a cost-benefit analysis.
    B. Discuss the breach expenses with legal.
    C. Review and audit your incident response plan.
    D. Provide the expenses to the CEO for their review.

46. The investigation of a company's latest data breach reveals that errors and negligence of several company employees were the breach's main cause. What is the best course of action for the company to reduce the probability of similar incidents in the future?

    A. Develop a comprehensive incident response plan.
    B. Terminate the employees responsible for the breach.
    C. Set up a company-wide awareness and training program.
    D. Purchase an insurance policy to cover the cost of remediation.

47. Which of the following is NOT set forth as a data protection officer (DPO) requirement under the GDPR?

    A. Access to the highest management level.
    B. Independent status to perform duties impartially.
    C. Ability to discipline any noncompliant employees.
    D. Adequately resourced to fulfil statutory responsibilities.

48. Which of the following best describes the benefits of a hybrid data governance model?

    A. Data privacy risks are evenly spread across each of the organization's departments.
    B. Common data processing goals are known and business units have some autonomy.
    C. Local managers lead the data privacy program based on their own areas of expertise.
    D. Data processes are uniformly streamlined across each of the business's departments.

49. Your organization, targeting individuals in the United States, is looking to implement a new customer relationship management solution, and you are on the project team in a privacy role. Under Ann Cavoukian's Privacy by Design principles, which item below would be most important when reviewing the collection of data to ensure that the answer is compliant with privacy regulations and principles before launch?

    A. Data minimization, to ensure that the collection of data is kept strictly to the minimum necessary.
    B. Integrity of data, to ensure that the data collected is a true and accurate representation of the users/community.
    C. Anonymization of data, to ensure that the data collected cannot be misused in the event of an incident or breach.
    D. Information security, to ensure that the collected data is secure within the solution and any associated databases.

50. What is the primary purpose of a vendor assessment?

    A. A vendor assessment helps to demonstrate the fulfilment of an organization's legal responsibilities.
    B. A vendor assessment helps ensure an organization safeguards itself from the vendor's own third-party risks.
    C. A vendor assessment helps determine whether the vendor works with any of the organization's major competitors.
    D. A vendor assessment helps determine whether the vendor can meet the organization's needs and identify potential risks.

51. Which of the following situations would NOT require conducting a privacy impact assessment?

A. Before anonymization of paper-based records via redaction.
B. Before a restructuring of the organization's management team.
C. Before the external launch of a new IT project, product or service.
D. Before a conversion of records from paper-based to electronic format.

SCENARIO VI

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

A global media company that operates through various outlets in fifteen countries and four continents is undergoing a global restructure. Traditionally, the business has operated in each country as a separate entity.

The business plans to pivot to a global structure to take advantage of economies of scale, streamlining teams and products and to create a unified customer database across all markets. Sharing data and information globally has increased risks to data privacy, and the global leadership team has recognized the need to create a global privacy program headed by a board-level chief privacy officer.

Prior to the restructure, there was no global privacy program, as each market operated its own privacy program with its own databases and systems. Personal data and processes were not shared across the global business between different markets or the global headquarters.

While the different markets are at varying levels of data privacy maturity, the new global CPO recognizes that each local market has data privacy teams with skills and knowledge pertinent to their region's regulatory environment and the local business unit's culture. The goal is to create global cross-functional teams operating at all levels of the business. Therefore, there is a strong need to create a new global data privacy vision from the start of the restructure to embed and instill a strong privacy ethic from the start.

The new CPO wants to operate a hybrid data governance structure that will harness some of the existing privacy programs but with a central global privacy team that defines the new privacy vision, who will communicate the new privacy program to the whole global business.

The new sales and marketing department will be based in the U.S. and will be responsible for global sales targets and growing subscriptions of the business's various subscription-based media products. The new global subscriber databases will also be based in the U.S., with current and prospective subscribers targeted in the global database and email marketing platform.

The business still has a privacy notice for each local market's websites, which does not describe the new way customer data is shared with different parts of the business in different countries, and each privacy notice is written to reflect the data privacy laws of that particular country. The business still has separate HR teams in each market with their own internal privacy policies.

A privacy program director has been recruited to the new global privacy team to support the CPO, and is responsible for communicating the new global privacy program across the business and running training and awareness programs.

52. One of the tasks of the privacy program director is to communicate about the privacy program to existing and prospective customers. Which of the following is the best way to create customer awareness of the privacy program?

    A. Put a video on the corporate website that outlines the vision or mission of the privacy program and links to local privacy notices.
    B. Employ a PR agency to run an awareness campaign of the new privacy program across various media platforms for a set period of time.
    C. Send an email to individuals in the database outlining the privacy mission with links to the local privacy notices that may affect them.
    D. Publish a global privacy statement that outlines the new mission with links to local privacy notices and notify existing customers of the change.

53. The new privacy team has identified that the global sales and marketing team, based in the U.S., requires additional privacy training and awareness. What is the best option to ensure they have access to the right policies, procedures and updates relative to their roles?

    A. Work with the local market data privacy team to create a training plan that they periodically review.
    B. Monitor the types of data privacy complaints sales and marketing receives and tailor training to address them.
    C. Provide the sales and marketing team with one-off training from an external company that specializes in data privacy.
    D. Add additional training modules specific to privacy to the standard training for newly hired sales and marketing employees.

54. The privacy director is working on a communications plan for the new privacy program. What is the best option for the privacy director to develop this plan?

    A. Cancel existing data privacy communications to make sure they do not contradict the new plan.
    B. Employ a communications agency that specializes in data privacy communications to help develop the new plan.
    C. Conduct employee research to find out the level of privacy knowledge to tailor the plan to the organization's needs.
    D. Engage with local data privacy teams to assess existing communications and schedule future communications.

55. Part of the privacy officer's role is to develop a new global privacy policy for the workforce. Which of the following would be the first action they should take to develop this?

    A. Gather existing privacy policies from all the HR departments for review.
    B. Draw up a global privacy policy and insert it into existing policy handbooks.
    C. Conduct employee focus groups to find out what they know in terms of privacy.
    D. Utilize the most data privacy-mature market to be the basis of policy development.

END SCENARIO VI QUESTIONS

56. If we consider the US market and an incident impacting US employees, which of the following is the one area that only lawyers can provide for the management of the incident?

    A. Decision to notify.
    B. Privileged conversation.
    C. Evidence Preservation.
    D. Exposure assessment.

57. Kelly is consulting for Switchwand Inc., a small company with limited resources, on risk management solutions. The CEO of the company is concerned that its financial position will limit options to secure the physical data collected and stored on location. Some safeguards are already in place, including scanning a keycard to enter the building and a clean desk policy. Kelly is responsible for the most cost-efficient way to protect files containing personal data. Of the below examples of physical security deterrents, which should Kelly suggest to Switchwand Inc. as the most cost-efficient option?

    A. CCTV cameras.
    B. Motion sensors.
    C. Locked filing cabinets.
    D. Smart-alert AI systems.

58. Justine has just been appointed data protection officer (DPO) of a tech start-up that produces a health monitoring app that is downloaded by users all over the world. As a new company, it is the first time they have had a DPO. What should her first task be?

    A. To review any existing privacy notices and update them.
    B. To download the app herself and test the various functions.
    C. To meet with her colleagues to discuss their privacy concerns.
    D. To understand the business goals and global reach of the company.

59. Which of the following is a best practice element regarding personal data breach management plans, but is not a legal requirement?

    A. Identifying whether a breach has occurred.
    B. Determining whether to notify impacted individuals.
    C. Notifying the police immediately upon discovery of a breach.
    D. Establishing organizational response roles when creating the plan.

60. What is the primary purpose of conducting a privacy threshold analysis?

A. Determine the level at which an organization is willing to absorb or mitigate risk during the exchange of information.
B. Assess the likelihood and severity of physical risks (e.g., natural calamity) to an organization during the exchange of information.
C. Identify what information will be exchanged, with whom it will be exchanged and whether there are any associated risks with its exchange.
D. Evaluate the level at which a privacy impact assessment affected an organization's capacity to absorb or mitigate risks during the exchange of information.

61. Which of the following is applied to continually monitor risks?

A. Controls.
B. Limitation.
C. Elimination.
D. Minimization.

62. You are hired as a privacy officer for an organization that collects sensitive personal data via a third-party vendor to provide a service to consumers. The organization is looking to embed privacy by design into its existing architecture. You are trying to figure out where to start. According to Ann Cavoukian's Privacy by Design Principles, which of the following is the most important consideration when approaching this issue?

A. Determine the needs and expectations of the individual users because they have the most vested interest in using and managing their personal data.
B. Create a data flow diagram to ensure that you are aware of all the various routes that collected personal data takes through the vendor and your organization.
C. Discuss the organization's own interests and uses for the personal data to ensure that any architecture keeps those needs at the forefront to meet business goals.
D. Examine the vendor's privacy and security practices to ensure that any personal data is safe while in the vendor's systems and when being transmitted to your organization.

63. A customer service agent accidentally sends an email to a customer containing information about another customer, which has not been password protected. The incident is escalated to the data privacy team. Which immediate step should the privacy team recommend the customer service agent take to mitigate the incident?

A. File an incident report with the with the appropriate privacy regulator or lead supervisory authority.
B. Contact the customer who received the information in error, ask them to securely delete it and confirm once done.
C. Contact the customer whose details were accidentally shared with another customer to inform them about what happened.
D. Send an updated, password-protected document containing the correct details to the customer who received the wrong information.

64. What should a privacy officer do before instituting processes or procedures?

A. Survey customers to determine what they find important.
B. Organize a workshop to identify risks, stakeholders and controls.
C. Research industry standards that and use them to create a PbD strategy.
D. Ask the board of directors in your organization what their goals are on privacy.

65. Ensuring the privacy program aligns with business initiatives is very important. Business units must know and understand the goals and objectives of the privacy program and be part of the solution. Which of the following is true when trying to achieve organizational balance and support in developing a privacy program?

A. Goals can best be met by incorporating strategies used by organizations in similar industries.
B. Compliance should be adjusted according to each team's preferences to ensure that teams can comply easily.
C. Goals must be fixed and only adjusted when a significant change affecting privacy occurs, such as a new regulation.
D. Compliance should be achieved with the least amount of business disruption while considering potential fines for noncompliance.

66. An unknown third party has managed to maliciously access a customer database containing large amounts of customer personal data records. No sensitive or special category data is known to have been affected. The response team has been notified and gathered. Which of the following should the team investigate first?

A. How many personal data records were affected.
B. Whether they know who is responsible for the attack.
C. Whether the customer database is properly encrypted.
D. Who in the business has knowledge of the customer database.

67. Which privacy governance model best allows an organization to function in a global environment yet maintain common missions, values, and goals, typically by dictating core values but allowing the employee to decide which practice to use to obtain those goals?

A. Local.
B. Hybrid.
C. Centralized.
D. Distributed.

68. Which of the following is an action an organization should take when developing a data retention policy?

A. Work with stakeholders to determine the business impacts of data deletion.
B. Work with IT to establish current data age and use as a base for retention plan.
C. Work with managers to develop and implement team-based data retention policies.
D. Work with the financial department to understand cost implications of data deletion.

69. Which of the following considerations comes after the development of a privacy program's scope and charter?

A. The type of business of the organization.
B. The roles and responsibilities of the privacy team.
C. The global geographic footprint of the organization.
D. Any applicable regulatory regimes and requirements.

70. As a result of a data breach involving a retail bank, the personal data of millions of the bank's customers was compromised. The data includes the customers' names, home addresses, employment details, bank account information and social security numbers. After the breach is contained, what remediation action would be the best for the bank to consider?

A. Appointing a dedicated full-time chief privacy officer.
B. Offering credit monitoring and identity theft insurance.
C. Encrypting all existing personal data in transit and at rest.
D. Issuing a press release with the details of the investigation.

71. A company uses a third-party agent to monitor their data subject requests. A new request is submitted by a different third-party website often used by individuals to help manage their digital footprints. How should the agent respond?

A. Provide the originator with a copy of the company's privacy notice.
B. Ignore the request since it was originated by a third-party website.
C. Remove the data associated with the email address without undue delay.
D. Reply to the originator requesting additional information to verify identify.

72. When assessing an artificial intelligence (AI) system, privacy principles are often hindered by the presence of AI. One such drawback is known as the "black box effect." This drawback refers to which of the following concepts?

A. A vast amount of information is needed to develop a particular AI function, making review difficult.
B. It is not always possible to explain why an AI model has generated a particular output or decision.
C. An AI system can be altered by predicting the system returns in response to new inputs at various times.
D. Intellectual property can be exposed when data subjects are informed about the algorithmic model that is being used.

73. Which of the following is a benefit of a centralized data governance model?

A. Data can be accessed quickly and easily.
B. Data processing compliance is guaranteed.
C. Data is handled consistently across the business.
D. Data is managed by each business unit independently.

74. You are the privacy officer for a large organization with multiple departments that historically have not communicated effectively with the privacy team. Which of the following is the best way to work toward integrating privacy representation across the organization?

A. Present the issue to the chief executive officer in detail so she can determine the best course of action moving forward.
B. Rely on a more stringent training and education program for all staff tied to professional goals and performance objectives.
C. Hire more staff for the privacy team who have department specific subject-matter expertise and introduce them to department heads.
D. Recruit and train individuals from departments, with manager approval, who will serve as privacy liaisons within those departments.

75. You are working at an organization that was recently served a class action lawsuit. The legal department has sent out a litigation hold for all records related to the impending matter. Your organization follows an information management policy that mandates keeping personal data for as long as operationally needed to meet business and legal obligations. The data relative to the lawsuit is no longer available. Through what process can you demonstrate that the organization follows a systematic destruction strategy?

A. Advise the legal department that the data has been appropriately destroyed.
B. Disregard the request as you do not have any data to which the request applies.
C. Conduct a data retention audit to demonstrate compliance with retention policies.
D. Contact affected departments to request emails confirming they could not find the data.

SCENARIO VII

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

After searching on the internet for vacation timeshares a few months ago, the number of timeshare advertisements continued to progressively populate on the family computer of Jared and Melissa Stark. After much hesitation, they decided to accept an offer from Marisol Multipropiedad, headquartered in Barcelona, Spain. With numerous properties throughout the Caribbean and other tropical locations around the world, Marisol Multipropiedad welcomed the Starks to one of their properties in Playa del Carmen, Mexico for a free four-night vacation if they supplied their own airfare. After Jared conducted a little research on the legitimacy of the company, they decided to accept the offer and began to provide Marisol Multipropiedad with a significant amount of personal data to secure the reservation, including contact information and financial details. Although one of the conditions of acceptance to the offer was to attend a day-long seminar and tour of the nearby time-share properties, the Starks needed a vacation and booked a flight from Denver, Colorado later that evening.

Roughly a month later, the Starks arrived in Cancun and were escorted to a passenger van with a few other couples and left the airport toward the vacation property 45 minutes south. The presentation for the time-share was scheduled for 9AM on Monday.

As Jared and Melissa entered the presentation room, they were each handed a tablet to begin filling out a questionnaire about spending habits, income and savings information, and which level and price range of timeshare ownership they were interested in with Marisol Multipropiedad. Secondly, they were directed to a different website for the actual resort, El Playacar del Mar, based in Playa del Carmen, Mexico, and asked to fill

out a variety of personal data (address, email address, generic financial information regarding their savings and investments). Neither the website nor the questionnaire contained a privacy statement.

Jared asked why he had to provide information when he had already given to Marisol. He was told that there may be limitations on access to that information, depending on the membership level they choose, and that smaller local companies may require information be provided directly to them.

Leaving the presentation, Jared and Melissa felt a little too pressured to purchase a timeshare membership at that time and planned to discuss matters when they returned home. Once home, the pressure to buy really intensified. Within weeks, both of their email inboxes were flooded with timeshare opportunities from an array of companies they had never heard of, but claimed to be a part of the Marisol Multipropiedad network, while others seemed to have no affiliation whatsoever. Pretty soon, offer after offer began arriving in the mailbox and telemarketing calls seemed to come at all hours. Jared finally had enough and decided to contact Marisol Multipropiedad to have them delete all of their personal information and to never be contacted again.

76. If Marisol Multipropiedad, based in Spain, wants to transfer Jared and Melissa's personal data to a smaller company, based in Mexico, how may it transfer the data?

    A. By using sectoral territory laws (STLs).
    B. By using a data transfer initiative (DTI).
    C. By using a standard contractual clauses (SCC).
    D. By using a certification mechanism found in Article 42.

77. How could Marisol Multipropiedad have avoided the concerns Jared raised regarding having to directly provide his information to other parties?

    A. By providing customers with their privacy notice.
    B. By providing customers with their privacy strategy.
    C. By providing customers with their privacy vision statement.
    D. By providing customers with their privacy mission statement.

78. What requirement under the GDPR did Marisol bypass regarding sharing personal data?

    A. Security.
    B. Consent.
    C. Availability.
    D. Documentation.

79. Jared no longer wants to receive any promotional/advertising emails from El Playacar del Mar. What affirmative action should he immediately take?

    A. Block or reject any "cookie consents" that appear on their website.
    B. File a formal complaint with their parent company, Marisol Multipropiedad.
    C. Go to their website and "unsubscribe" to any future contact with El Playacar del Mar.
    D. Create a "dark pattern" to show his consent to opt-out of receiving additional promotions.

END SCENARIO VII QUESTIONS

80. Who is responsible for determining how frequently the intended objective of the organizational vision for privacy should be reviewed?

A. The IT department head.
B. The chief executive officer.
C. The in-house legal counsel.
D. The data protection officer.

81. A Europe-based company (Company A) agrees to acquire a startup company (Company B). Company A decides to assess the maturity of Company B's privacy processes. In the assessment, it finds that procedures and processes are fully in place, they are fully documented and they cover the scope of expected controls; however, Company A cannot find any evidence of reviews to assess the effectiveness of the controls. Under the privacy maturity model (PMM), Company B should be considered at which level of maturity?

A. Defined.
B. Managed.
C. Optimized.
D. Repeatable.

82. A company operating solely in the U.S. has a notice in its rules of conduct for employees that their internet usage will be monitored to ensure the use is appropriate and necessary to the performance of their job. When analyzed in light of privacy by design compliance, which of the following is correct about the rule?

A. The rule is appropriate if combined with other measures, such as ensuring that all records are securely stored and disposed and only individuals with a need to know have access to such records.
B. The rule is inappropriate if it is considered a work requirement for the user to sacrifice their privacy, which goes against the positive sum/zero sum principle—an important component of privacy by design.
C. The rule is inadequate considering that privacy is an absolute individual right, which cannot be delegated and inseparable, and any codes of conduct that interfere with the personal right to informational self-determination are irregular.
D. The rule is inappropriate if the user is informed in a transparent manner that the use of company devices makes any expectation regarding privacy unfeasible in order to preserve the confidentiality, integrity and availability of company information.

83. Due to a legislative amendment, an organization's lawyers recently updated its privacy policy to include additional uses of personal data. As the privacy officer, you are unsure of how the changes affect your current program. How do you confirm that your privacy program remains compliant with the privacy policy?

A. Audit the policy against the privacy management program to determine if there are gaps.
B. Compare the language of both policies to determine what the differences are between them.
C. Wait until you receive a complaint that will trigger a review, then review the specific concern.
D. Speak to the legal department to determine if the privacy program complies with the updates.

84. In which of the following situations is an organization NOT required by the General Data Protection Regulation (GDPR) to designate a Data Protection Officer (DPO)?

A. Where the organization is a public authority or body processing data on a large scale in multiple countries.
B. Where the organization is a court or independent judicial authority processing data on a large scale in its judicial capacity.
C. Where the core activities of the organization consist of processing on a large scale of personal data relating to criminal convictions and offences.
D. Where the core activities of the organization consist of processing operations that require regular and systematic monitoring of data subjects on a large scale.

85. Company A, located in Germany, decided to change processors from OldPay to NewPay for its payroll services, which includes tax reporting. Once all personal data is transferred from OldPay to NewPay, which of the following determines when OldPay must delete the records?

A. Contractual agreements between Company A and OldPay.
B. Contractual agreements between Company A and NewPay.
C. Confirmation from NewPay that they have received all records.
D. Compliance with the shortest applicable statutory requirements.

86. When developing an effective internal communications plan, the privacy program management team needs to address each of the following questions EXCEPT which of the following?

A. Should there be a recurring time slot assigned on the communications calendar dedicated to particular messaging?
B. Is a communication necessary or can the messaging be covered in more dedicated guidance documents or training?
C. What methods, such as meetings, phone calls and conference calls will the privacy team use to work with human resources?
D. Has the privacy team conducted a privacy workshop or training for stakeholders to define privacy for the organization and reduce confusion?

87. What is the difference between a key risk indicator (KRI) and a key performance indicator (KPI)?

A. There is very little difference. KRIs and KPIs both act a metrics for changes in an organization's risk profile in respect of people, threats, vulnerabilities and impact, leading some organizations to use the terms interchangeably.
B. KPIs are more generalized than KRIs. KPIs provide a high-level overview on how a company is performing as well as analytics on trends in general performance, while a KRI evaluates one indicator of performance for future improvement.
C. KRIs help to broadly quantify risk to determine an organization's risk-benefit portfolio and return on investment. However, KPIs evaluate past performance indicators and are more specific and can also be used in a report on KRIs.
D. A KRI is a metric that helps monitor, analyze, manage and mitigate risks, threats, vulnerabilities and the impact they may have on the performance of a business. By contrast, a KPI illustrates how efficiently an organization is meeting its goals and objectives.

88. VendorZ is a small third-party vendor that handles XCompany's payroll through a contractual arrangement wherein XCompany maintains control of how the data is processed. XCompany has expanded significantly, so VendorZ wants to use ABCVendor, a larger company, to help VendorZ process XCompany's payroll. What step must VendorZ take, after proper vetting, before transferring payroll processing to ABCVendor?

    A. Inform XCompany's employees of the payroll change.
    B. Process the transfer immediately after internal approval.
    C. Notify their point of contact at XCompany of the transfer.
    D. Provide details of the transition to supervisory authorities.

89. Which of the following skills and qualifications are most important for a privacy manager to be effective in any size organization?

    A. Previous experience managing privacy programs as a data protection officer.
    B. Ability to learn and improve the privacy program through day-to-day experiences.
    C. Multiple certifications in privacy program management and related security practices.
    D. Legal background to provide legal guidance to the organization during incident investigations.

90. Which of the following is an assessment mechanism for controllers to assess the reliability of a processor?

    A. Copies of the processor fiscal reports pertaining to the previous fiscal year as prepared by an authorized accountant.
    B. A reliable consumer reporting agency (CRA) report exhibiting the processor creditworthiness and compliance.
    C. Press reports regarding the processor participation in public auction procedures and allocation of public services contracts.
    D. Audit observations to ensure that the processor implements and maintains appropriate technical and organizational measures to secure the data.

Answer Key

For each correct response, place a "1" or a checkmark in the corresponding domain column (white space).

Note: the domain is 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*
1	C				*C*								
2	C						*A*						
3	D								*C*				
4	A												*B*
5	B										*A*		
6	B		*A*										
7	D				*D*								
8	A												*C*
9	A										*B*		
10	C						*B*						
11	D												*A*
12	A		*A*										
13	A		*C*										

Item Number	Correct Answer	Domain I	*Competency*	Domain II	*Competency*	Domain III	*Competency*	Domain IV	*Competency*	Domain V	*Competency*	Domain VI	*Competency*
14	C				*D*								
15	A								*A*				
16	A												*A*
17	D												*A*
18	B				*B*								
19	C								*A*				
20	A						*D*						
21	B				*A*								
22	B						*B*						
23	A												*B*
24	B								*A*				
25	C										*C*		
26	B		*A*										
27	C						*A*						
28	D		*C*										
29	B										*C*		

Item Number	Correct Answer	Domain I	*Competency*	Domain II	*Competency*	Domain III	*Competency*	Domain IV	*Competency*	Domain V	*Competency*	Domain VI	*Competency*
30	B								*C*				
31	B								*C*				
32	D		*A*										
33	B						*E*						
34	C						*E*						
35	D				*C*								
36	A												*B*
37	C		*A*										
38	A						*D*						
39	D						*C*						
40	A								*C*				
41	A								*C*				
42	A		*A*										
43	B												*A*
44	A						*A*						
45	A												*C*

Item Number	Correct Answer	Domain I	*Competency*	Domain II	*Competency*	Domain III	*Competency*	Domain IV	*Competency*	Domain V	*Competency*	Domain VI	*Competency*
46	C				*D*								
47	C				*A*								
48	B		*A*										
49	A								*B*				
50	D						*B*						
51	B						*E*						
52	D												*A*
53	A		*B*										
54	D		*B*										
55	A		*B*										
56	B				*B*								
57	C						*C*						
58	D		*A*										
59	D				*A*								
60	C						*A*						
61	A								*A*				

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

Item Number	Correct Answer	Domain I	*Competency*	Domain II	*Competency*	Domain III	*Competency*	Domain IV	*Competency*	Domain V	*Competency*	Domain VI	*Competency*
78	B												*A*
79	C												*A*
80	D				*B*								
81	A						*A*						
82	A								*B*				
83	A										*B*		
84	B		*C*										
85	A						*B*						
86	C								*A*				
87	D				*C*								
88	C						*B*						
89	B		A										
90	D						*B*						
SUMMARY		___ of 18 correct		___ of 14 correct		___ of 20 correct		___ of 15 correct		___ of 6 correct		___ of 17 correct	
PERCENTAGE (# correct/# total) x 100													

Item Rationales

1. The correct answer is C. A maturity assessment can be used to measure the current maturity level of a certain aspect of an organization in a significant manner, enabling stakeholders to clearly identify strengths, improvement points and accordingly prioritize what to do to reach higher maturity levels.
   Body of Knowledge Domain II, Competency C

2. The correct answer is C. Measure and control processes to establish effectiveness. Under the maturity level of "defined," a privacy program should already have procedures and processes fully documented and implemented. To move to a "managed" level, it should also conduct reviews to assess the effectiveness of the controls in place.
   Body of Knowledge Domain III, Competency A

3. The correct answer is D. How and when employees may utilize work devices for personal communication is a privacy matter that could be addressed with an HR policy. If employees are permitted to use work devices for personal communication, there should be a policy which outlines any monitoring that may occur and under what circumstances personal usage might not be private. While the other items listed may be HR concerns, they are not privacy matters.
   Body of Knowledge Domain IV, Competency C

4. The correct answer is A. Not all incidents are reportable breaches. Requirements to report a data incident differ from jurisdiction to jurisdiction, from country to country and even from one part of the country to another (e.g., the different states within the United States). Determination of a breach and, when applicable, the resultant breach notification process depend on many factors, such as the amount and nature of data compromised, the impact on the affected individuals, the steps the company took to address the breach and many others. Before any action is taken, the company should reach out to the appropriate response team for the appropriate next steps.
   Body of Knowledge Domain VI, Competency B

5. The correct answer is B. The irregular component does not use trending analysis when reporting data that focuses on data patterns over a given time period nor does it use tracking data over a period of time with a set of regular fluctuations, known as the cyclical component. The irregular component, which is the most difficult to detect, focuses on the data that is left over or the absence of data after the other variables of the equation (time and cyclical) have been factored.
   Body of Knowledge Domain V, Competency A

6. The correct answer is B. It is most critical to align privacy governance documents with a company's business objectives (to include all locations, subsidiaries, etc.,) for the program to be successful. Once these foundational

documents have been developed to ensure congruence with the company's mission, vision and values, the work to analyze laws and regulations in scope, build relationships with primary regulators, etc., then begins.
Body of Knowledge Domain I, Competency A

7. The correct answer is D. It is important for a company's privacy management program to be tailored in line with the company's governance structure. Since this company's focus is on decentralized governance and management of decision-making at the local level, the most appropriate choice for effective training should be to allow privacy professionals to train employees locally if possible.
Body of Knowledge Domain II, Competency D

8. The correct answer is A. Each of the listed considerations are important at various stages of privacy management; however, only "Understanding key stakeholders and managing vendors" is a category of incident preparedness. Incident preparedness will not prevent a breach or privacy incident; rather, it allows an organization to respond in an appropriate manner when an incident occurs. The other three considerations are: training, having an incident response plan and getting insurance coverage where appropriate.
Body of Knowledge Domain VI, Competency C

9. The correct answer is A. Of the three plausible and defined types of audits (a standardized audit does not exist), a supplier audit, or second-party audit is an agreement where the supplier functions as if they are part of the organization. This contractual agreement should include language with specific privacy and regulatory requirements and require evidence of compliance.
Body of Knowledge Domain V, Competency B

10. The correct answer is C. While reviewing the contract, including termination procedures is important and location may play a role in selecting a vendor, out of these options, only the reputation of the vendor should be a standard for initial consideration. Review available feedback about the vendor with reputable sources, including supervisory authorities, to assess the vendor's reputation. This will allow you to avoid vendors who have had consistent issues adhering to or maintaining proper privacy procedures.
Body of Knowledge Domain III, Competency B

11. The correct answer is D. To process personal data, some jurisdictions have laws and/or regulations requiring organizations that collect the data to obtain consent from data subjects. If consent is required, an organization should have processes and procedures in place to obtain consent and record it. While giving their consent, a data subject is expected to read the privacy notice published on the website at the time the consent is given. Privacy notices are living documents that are updated periodically, for example, due to new laws or regulations or changes in the company's data processing practices. Hence, the record of consent should be kept along with the privacy notice provided to the data subject at the time consent was obtained. Such practice will help organizations clarify misunderstandings raised by data subjects and have proof at hand in the form of the privacy notice provided to them at the time of obtaining their consent. Storing the privacy notice provided to the

patients along with the record of their consent will also help the organization defend against potential legal claims.
Body of Knowledge Domain VI, Competency A

12. The correct answer is A. Data governance is the process of identifying the vital data belonging to an organization and making sure it is secure and that data quality is maintained. It should include processes, policies, roles, metrics and standards to ensure the effective and efficient use of the organization's data in its entirety.
Body of Knowledge Domain I, Competency A

13. The correct answer is A. When functioning globally on a macro level, organizations must employ representatives in various geographic regions to ensure that the business functions appropriately on a micro level, such as ensuring that proposed privacy policies, processes and solutions align with local laws are monitored at the local level to ensure ongoing compliance when changes occur locally.
Body of Knowledge Domain I, Competency C

14. The correct answer is C. Through her interviews, Betty has discovered there are gaps in employees' privacy awareness knowledge across the company. This lack of knowledge presents a privacy risk for the company. Employees at all levels in an organization should understand the basic laws, regulations, policies and procedures that set out the organization's requirements for handling personal data.
Body of Knowledge Domain II, Competency D

15. The correct answer is A. During the privacy operational life cycle, information security controls can be implemented to manage risks. These can be divided into three categories: physical controls (fences, doors, locks), administrative controls (processes, policies, training and awareness) and technical controls (two-factor authentication, encryption, firewalls, etc.).
Body of Knowledge Domain IV, Competency A

16. The correct answer is A. The company should consider obtaining a letter of authority or other documentation to show evidence that Mollie has given the legal representatives permission to act on her behalf and receive the information from the retailer as part of her data subject access request. If she has given permission for information to be shared with her legal representative, the company should not withhold it or provide it only to Mollie. It is important to validate a third party's authority to act on behalf of an individual to avoid supplying the information to an unauthorized party and potentially causing a data incident.
Body of Knowledge Domain VI, Competency A

17. The correct answer is D. Mollie is not entitled to information that would disclose how the company assigns account managers, as this would potentially give away confidential operational information about the business. She would be entitled to the other information as part of her request.
Body of Knowledge Domain VI, Competency A

18. The correct answer is B. The role of the ethics and compliance department is to respond to complaints about how personal data is being handled. The department should review all complaints and ensure personal data is being handled in accordance with the company's privacy policy and notice. In addition, the department may be tasked with informing the privacy or legal teams when it receives repeated, related complaints about how personal data is used even if such uses are compliant with the policies and notices, especially when dealing with consumers. Public opinion matters, and unless such processing is vital, consistent negative feedback may indicate a change is needed.
Body of Knowledge Domain II, Competency B

19. The correct answer is C. When creating privacy-centric policies for the organization, high-level policies may dictate organizational expectations across departments, while additional policies and procedures can address the needs of the organization to serve a specific purpose.
Body of Knowledge Domain IV, Competency A

20. The correct answer is A. The Article 29 Working Party Section III provides a more concrete set of processing operations that require a DPIA due to their inherent high risk:
    - Evaluation or scoring
    - Automated decision-making with legal or similar significant effect
    - Systematic monitoring
    - Sensitive data or data of a highly personal nature
    - Data processed on a large scale
    - Matching or combining datasets
    - Data concerning vulnerable data subjects
    - Innovative use or application of new technological or organizational solutions, such as the combined use of fingerprints and face recognition for improved physical access control.
    - When the processing prevents data subjects from exercising a right or using a service or a contract

    Body of Knowledge Domain III, Competency D

21. The correct answer is B. A data inventory or data flow map shows how data moves within an organization. The data inventory will show how personal data is handled from the point it is collected, accessed and used, where and how it is stored, and who it is shared with externally.
Body of Knowledge Domain II, Competency A

22. The correct answer is B. Under many privacy laws, organizations are liable for their vendors' processing activities. By assessing vendors' privacy practices through questionnaires, privacy impact assessments and reviewing the vendor's policies, an organization can reduce potential fines as well as risk to its reputation and data subjects.
Body of Knowledge Domain III, Competency B

23. The correct answer is A. The data affected was that of the employees of the supermarket. Since each clients' data is kept separate and there were no indications that other clients' data was affected, there is no need to notify them. However, there is the possibility that other supermarket employee data was also affected. It is prudent to inform all those who might be impacted about the breach. In addition, all employees should be informed so if they receive inquiries from the public, they are equipped to respond to those queries.
Body of Knowledge Domain VI, Competency B

24. The correct answer is B. While contracts are important to ensure proper handling of personal data, especially when data needs to be removed, added or when a relationship is terminated, they are not typically a contributing factor to minimizing the effect of a data breach.
Body of Knowledge Domain IV, Competency A

25. The correct answer is C. Technology changes rapidly and existing products and processes may be affected by updates and patches, which may introduce new risks. It is necessary to review privacy impact assessments when changes are made to existing technology, as well as when new technology is introduced, to ensure the changes have not created additional or unexpected risks.
Body of Knowledge Domain V, Competency C

26. The correct answer is B. The executive sponsor is responsible for making sure that the organizational vision and goals for privacy align well with the overall company strategy. This helps gain support for the privacy activities within the organization.
Body of Knowledge Domain I, Competency A

27. The correct answer is C. A privacy threshold analysis is conducted to determine which systems need a privacy impact assessment (PIA), thus should be completed prior to the PIA.
Body of Knowledge Domain III, Competency A

28. The correct answer is D. Complying with each applicable and potential privacy law can give rise to significant operational and budgetary challenges; even though privacy laws in different states and countries are very similar, there are slight but important differences, which may make implementation of a privacy program complex and costly. A privacy program should consider all information gathered by an organization and the legal requirements for that information, based on where and how information is being gathered and processed.
Body of Knowledge Domain I, Competency C

29. The correct answer is B. The audit lifecycle begins at the planning stage, followed by the preparation, audit, reporting and follow up phases. Note that while these are the standard recognized phases, some stages may be repeated or omitted in any given cycle.
Body of Knowledge Domain V, Competency C

30. The correct answer is B. HR deciding who has access to the data is a good way to impart responsibility and control of data access. Line Managers should only be able to view the data belonging to their direct reports and not of other employees in the company. Data should be limited to what is needed to fulfil a purpose and, in this scenario, there is no reason a Line Manager would need to view data belonging to an employee who does not report into them. The same goes for the entire HR team; maybe some specific HR employees could be involved for the purpose of rolling out the survey. There is no reason the data privacy team should need to access actual and real data in order to carry out a Data Protection Impact Assessment.
Body of Knowledge Domain IV, Competency C

31. The correct answer is B. The words 'automatically' and 'analyzed' indicates there could be some use of artificial intelligence or automated decision-making during the collection of the information, before it is presented to line managers. There is an increased use of this type of technology, which privacy professionals need to be aware of and take into account during the vendor due diligence process. Additional assessments may need to be undertaken, such as a Data Protection Impact Assessment. The volume of employees does indicate a higher amount of data, however, is not necessarily on its own a concern. With the identification of employees on an individual level, a recommendation may be to look at anonymity or viewing results at a team level, however this again may not be particularly high risk. Finally, line managers having access to the platform enables the access controls intended and is usually a preferred option rather than sending the data through potentially unsecure means (e.g. email), providing technical safeguards have been applied and accepted by the company.
Body of Knowledge Domain IV, Competency C

32. The correct answer is D. Obtaining buy-in from executives and the required support, including financial support, is the key to the success of any privacy program—especially in situations of budgetary constraints—so that key stakeholders are aware of the importance of such work.
Body of Knowledge Domain I, Competency A

33. The correct answer is B. The security of the already combined dataset, the review to ensure legitimate processing and the potential processing of healthcare data were risks already created by the pooling of the marketing data by GoodSnack. The use of AI on the dataset by SnackAI to create customer-specific pricing gives a new challenge to the transparency of processing. The so-called "black box" processing often used in AI can make it difficult to document and track how decisions are made.
Body of Knowledge Domain III, Competency E

34. The correct answer is C. The requirement for a data protection impact assessment (DPIA) is triggered when there is a high risk to the rights and freedoms of the individuals whose data has been processed. The number of European jurisdictions whose citizens' data is being processed does not change the risk to the individuals. The presence of financial data and/or the volume of data present increases the risk but would not directly trigger a DPIA. However, where profiling is used and this use leads to decisions of legal effect or similar, the WP29 issued clear guidance that this would trigger the requirement for a data protection impact assessment.
Body of Knowledge Domain III, Competency E

35. The correct answer is D. There is no defined lifespan for a privacy impact assessment/data privacy impact assessment (PIA/DPIA), but it is good practice to review PIAs at regular intervals to ensure they remain accurate and the risks have not changed. The frequency of review should be based on the risk of the processing activity. The higher the risk, the more frequent the review.
Body of Knowledge Domain II, Competency C

36. The correct answer is A. Attempting to keep information about a breach from employees is generally not practical, particularly where there is a reputational risk to the company or where notification of affected individuals is required. To minimize the chance of gossip or misinformation, an employee-only communication may be useful to address any questions that are likely to arise.
Body of Knowledge Domain VI, Competency B

37. The correct answer is C. Designing the scope of a privacy program follows the establishment of a privacy mission or vision statement and relies on the organization's ability to identify the specific privacy and data protection laws and regulations that apply to it. To be able to determine its regulatory obligations and thus the scope of the privacy program it will have to adopt, the organization must first identify which personal data is being collected, used, stored and otherwise processed.
Body of Knowledge Domain I, Competency A

38. The correct answer is A. Under the transparency principle, the employees of Company Z should be made aware of how Company X will process their data at the point of processing. Accuracy of data is an important privacy principle, but it does not negate the importance of other principles, including transparency. While testing on live data presents privacy challenges that need to be addressed, it is not specifically prohibited.
Body of Knowledge Domain III, Competency D

39. The correct answer is D. Privacy program management programs include administrative, technical and physical controls. Understanding the categorization of each control will help you respond appropriately to assurance requests. Clean desk policy, locked cabinets, access-controlled entry and power down of office computers are all processes that can be undertaken to help ensure personal data in physical form is protected from unintended or malicious access.
Body of Knowledge Domain III, Competency C

40. The correct answer is A. Access to an organization's information systems should be tied to an employee's role. No employees should have greater information access than is necessary to perform their job functions. An access control policy should be established, documented and reviewed based on business and security requirements for access.
Body of Knowledge Domain IV, Competency C

41. The correct answer is A. While an understanding of legal impacts, types of requests and the technical processes for compliance may be helpful, none of them are vital to the efficient and consistent process for handling data

subject complaints. However, knowing how to authenticate data subjects according to set guidelines is necessary to ensure that the process is consistent and runs smoothly.
Body of Knowledge Domain IV, Competency C

42. The correct answer is A. Privacy frameworks are the structure on which program management is built. It gives a bird's-eye view of all the processes and programs in place. By implementing a privacy framework, a business can ensure it is not only adhering to the requirements of legislation, but that it is taking appropriate and comprehensive steps to protect the personal data it processes on behalf of individuals.
Body of Knowledge Domain I, Competency A

43. The correct answer is B. Consent is the foundation of privacy law. Obtaining explicit consent from an individual is sufficient in demonstrating consent for the collection and use of personal data. Ensuring that an opt-out mechanism is established and functioning as intended is sufficient in further demonstrating compliance with withdrawal of consent requirements.
Body of Knowledge Domain VI, Competency A

44. The correct answer is A. Having up-to-date records of personal data that are under an organization's control is not only a best practice that allows the organization to keep track of the data it processes, but also an obligation under some of the personal data processing regulations around the world. Knowing the flow of data enables organizations to address data requests as well as comply with the various legal requirements for data privacy. When a new personal data processing vendor is engaged, updating the data processing inventory (also known as a data map) will help the organization identify the data and take action when and if needed. Sending the agreement with the vendor to all customers or informing the regulator of the new vendor are not required and likely will not promote better data practices with the new vendor. Assessing a vendor's risk appetite may be helpful to determining whether or not you want to contract with them; however, this should be done prior to signing the agreement with the new vendor.
Body of Knowledge Domain III, Competency A

45. The correct answer is A. A detailed cost-benefit analysis should include specifics about instituting risk assessment and mitigation plans, as well as an incident response plan. Showing how these two processes can minimize the data affected in the event of a breach, thereby reducing both risk and cost, and potentially reduce any fines incurred will show the benefit of having these processes in place once you compare the cost of instituting these measures to the expenses incurred in the recent breach.
Body of Knowledge Domain VI, Competency C

46. The correct answer is C. Statistically, employee error and negligence have been found to be one of the major contributing factors to personal data breaches and security incidents. Therefore, to decrease the risk of such incidents, having a robust privacy program is imperative for any company protects the privacy and security of personal data it processes. Privacy awareness starts at the highest levels of an organization and cascades down to all its staff. Depending on the role, different employees would likely need different training. The idea is to instill a company-wide personal data awareness mindset and empower employees to make decisions and take

actions accordingly. Since the incident described in the scenario can be traced back to errors and negligence of several of the company's employees, setting up a company-wide awareness and training program or refreshing the current one (if one existed) would be the best course of action for the company to take to reduce the probability of similar incidents happening in the future.
Body of Knowledge Domain II, Competency D

47. The correct answer is C. As defined in the GDPR Article 38, the DPO shall be supported in performing their tasks, report directly to the highest management level and not receive instruction regarding the execution of their tasks. There is nothing in the GDPR about the authority of the DPO to fire employees.
Body of Knowledge Domain II, Competency A

48. The correct answer is B. Hybrid governance models utilize both the centralized and local governance models to fulfill common privacy goals of the organization. The processing goals are known and shared, but business units have some autonomy in how they achieve those goals. Decentralized units are tasked with determining the best way to fulfil these goals. A central governing body supports the business units by issuing policies to address the level of privacy risk.
Body of Knowledge Domain I, Competency A

49. The correct answer is A. Item 2 in Privacy by Design principles, as written by Ann Cavoukian, recommends "Privacy as the Default Setting" in systems. Several Fair Information Practices (FIPs) inform default settings for privacy programs, including purpose specification, collection limitation, data minimization, and use, retention, and disclosure limitations, all of which strict privacy-protective controls. In this case, since no other FIPs are included in the options, the best option is data minimization, the principle that only the strict minimum of information is collected from individuals.
Body of Knowledge Domain IV, Competency B

50. The correct answer is D. Vendor assessments are an important step in the procurement process as it helps a business ensure that they are working with vendors that can meet the company's needs. It also helps an organization better understand the processor and vendor's capabilities and any potential risks that might come with working with that third party.
Body of Knowledge Domain III, Competency B

51. The correct answer is B. A privacy impact assessment (PIA) evaluates privacy implications when information systems are created or when existing systems are significantly modified, and as such it needs to be accomplished prior to the deployment of a project, product or service so to suggest or provide remedial actions or mitigations necessary to avoid or reduce/minimize those risks. It is not necessary to conduct a PIA when restructuring personnel in an organization.
Body of Knowledge Domain III, Competency E

52. The correct answer is D. The privacy program is ongoing, so all prospective customers need access to information regarding the organization's privacy mission and vision; therefore, a privacy notice is the best way to do this compared to a one-off email. A corporate website in a large organization with many customer-facing websites would not reach as many people as having a unified privacy statement across all privacy notices. An awareness campaign would also not have the lifespan of a statement permanently linked to all websites. The organization could have a single privacy notice on all websites, but with a hybrid model where each country has some elements of its privacy program, a global privacy statement with local privacy notices is best.
Body of Knowledge Domain VI, Competency A

53. The correct answer is A. Working with the sales and marketing team's local privacy team means there are privacy experts close to them who can work on an ongoing training plan that is periodically reviewed and updated to make sure it matches the needs of the sales and marketing team. Privacy programs should be created to prevent data protection breaches, complaints, etc., and the program should be proactive rather than reactive; a data protection authority would not look kindly on an organization that only trained staff after a problem occurred and did not have an adequate training program established to anticipate what problems may arise. While a training company could be utilized, a one-off training session will not address changes as they arise and will not include new employees. Lastly, even if the additional training modules are adequate, the option does not include the existing sales and marketing team, only employees new to the team.
Body of Knowledge Domain I, Competency B

54. The correct answer is D. As the data governance structure is a hybrid structure with local market data privacy teams, they will already have communications in place that may be suitable to the new privacy program. To develop a plan, the privacy director should gather these communications to review and assess what can be kept in the plan and what should be changed.
Body of Knowledge Domain I, Competency B

55. The correct answer is A. Reviewing current policies and procedures from HR allows a new global policy document to be created based on this knowledge. Additionally, a privacy officer must consider local data privacy and HR rules and regulations.
Body of Knowledge Domain I, Competency B

56. The correct answer is B. The legal department is likely to be involved in any decision to notify, based on facts presented. Legal will also likely provide input into any exposure assessment along with business partners like corporate communications, HR and IT/security, not independently. The Information technology function is likely to lead on evidence collection but again this could be supported through legal and their external partners. The correct answer is privileged conversation. The presence of a lawyer within the incident management team will allow some conversation to take place under legal privilege, meaning, these conversations are potentially NOT subject to legal discovery if the incident ends in a court case.
Body of Knowledge Domain II, Competency B

57. The correct answer is C. Privacy-enhanced or privacy-focused solutions vary in functionality, technical specifications and cost. The responsibility of protecting and safeguarding personal data belongs to the organization, regardless of the availability of resources. When physical files are involved, a simple solution may work best: lock the files away when not in use. To enhance security, additional cost-effective safeguards can be employed, such as limiting who has access to the keys or having the files stored in a room requiring an additional keycard scan for access.
Body of Knowledge Domain III, Competency C

58. The correct answer is D. A full understanding of the business goals and the global reach of the company will enable her to determine which laws apply within and beyond the privacy arena. For example, HIPAA may be relevant if there are customers in the U.S. Once she has that understanding, she can meet with her colleagues to discuss their privacy concerns and review existing privacy notices. There is no need for her to download the app herself.
Body of Knowledge Domain I, Competency A

59. The correct answer is D. Establishing roles in advance of a personal data breach is not a requirement described in the GDPR or other regulations, but it is a best practice which allows an organization to respond appropriately and more quickly when a breach occurs.
Body of Knowledge Domain II, Competency A

60. The correct answer is C. A privacy threshold analysis is used to determine if an information technology system contains personal data and whether a PIA is required. It will also help determine what other privacy requirements apply to the processing of that data.
Body of Knowledge Domain III, Competency A

61. The correct answer is A. Information security ensures the confidentiality, integrity and availability of information from the time the data is created or collected to the time of its destruction. Throughout the data lifecycle the information security team may be continually monitoring risks as the combination of an event and its consequence by applying appropriate controls to manage risk.
Body of Knowledge Domain IV, Competency A

62. The correct answer is A. The most important aspect of privacy by design (PbD) is to keep the user's needs at the forefront of all other considerations. While organizational interests, security practices and data flows are essential, the most crucial part of PbD is to respect the user's privacy and to keep any architecture and use of personal data "user-centric" by following the Fair Information Practices of consent, accuracy, access, and compliance.
Body of Knowledge Domain IV, Competency B

63. The correct answer is B. Contacting the customer who received the information in error and securely deleting the information is a best practice and one that should be performed immediately to mitigate any further exposure or use of that information by third parties who are not authorized to view it
Body of Knowledge Domain VI, Competency B

64. The correct answer is B. Before instituting processes and procedures, a privacy officer needs to identify the risk and the internal stakeholders and then identify the controls. Doing so helps to ensure that existing controls are taken into consideration and all concerns are raised by the necessary parties.
Body of Knowledge Domain IV, Competency A

65. The correct answer is D. When instituting a new privacy program or adjusting an existing one, organizations should try to minimize the disruption to the existing business processes. However, some disruption may be necessary to ensure compliance with privacy requirements.
Body of Knowledge Domain I, Competency C

66. The correct answer is C. It is important to establish whether the customer database in this scenario was properly secured. An unsecured database could increase the risk that more data could be exposed, meaning that customer information could be placed at further risk. While it is important to understand how many personal data records have been affected, it is not an initially critical question that needs to be answered, as volume alone may not necessarily trigger the reporting threshold—unless, for example, it was combined with particularly sensitive datasets that may cause individuals harm. It is not important at this stage to know who in the business had knowledge of this database, although this might help establish the extent of the data that existed within it. Finally, as an unknown third party maliciously carried out the attack, it is not critical at this stage to find out precisely who may have done it. Sometimes, you never truly find out.
Body of Knowledge Domain VI, Competency B

67. The correct answer is B. Local and distributed privacy governance models are both types of decentralized governance models. In a decentralized model, decision-making is delegated down to lower levels of the organization structure. This is considered to lead to less rigid policies with limited global consistency. A centralized approach will dictate both the core values and how these should be achieved. A hybrid model, as the name suggests, uses aspects of both centralized and decentralized models, allowing for some control without being overly rigid.
Body of Knowledge Domain II, Competency B

68. The correct answer is A. Data retention and deletion guidelines should be assessed according to the organization's legal and business requirements, which requires working with stakeholders to develop policies. Having a policy that states when specific data should be deleted and having procedures in place to ensure the policy is followed helps prevent over retention of unnecessary data, reducing risk to both the data subjects and the organization.
Body of Knowledge Domain III, Competency D

69. The correct answer is B. The structuring of the privacy team, and identification of roles and responsibilities, can only be conducted after the development of the privacy program's scope and charter, given that the identification of roles and responsibilities stem from the needs of the privacy program itself.
Body of Knowledge Domain II, Competency B

70. The correct answer is B. Responding to a data breach is a multi-step process. Planning for the breach before it happens, handling the breach while it is in progress, and remediating the breach's impacts after it's contained are the three main components of the process. With the nature of personal data compromised (names, home addresses, employment details, bank account information, and social security numbers), there is risk to the credit score and of identity theft to individuals affected by the breach if their data is used by bad actors. Therefore, of the choices provided, offering credit monitoring and identity theft insurance is the best remediation action for the bank to consider. Encrypting personal data is a data processing best practice; however, it's part of the prevention efforts rather than remediation, as asked by the question. Appointing a chief privacy officer (CPO), if one did not already exist, is another example of a proactive organization and indicates a company that takes privacy seriously. However, merely appointing a CPO would not remediate the damage to the bank customers, nor will it reduce the risk of their personal data being maliciously used. Issuing a press release with the details of the investigation is typically done as a part of the ongoing updates the bank would do while the incident is still ongoing.
Body of Knowledge Domain VI, Competency B

71. The correct answer is D. Properly responding to data subject access requests is essential for every business to avoid unnecessary scrutiny. This, however, does not mean that the business should blindly honor any and every request to remove personal data. Nowadays, when so many automated third-party web tools are available to process data subject requests, caution should be taken regarding handling these requests. To ensure the request is genuine, the agent should confirm the requestor's identity prior to disclosing information. Failure to do so could result in a data breach.
Body of Knowledge Domain VI, Competency A

72. The correct answer is B. A "black box algorithm" is one in which the processes are hidden from the data subject. The data subject has no way of knowing how specific end results were arrived at as the specific processes are not disclosed. At times, even those using the system may not know the processes and algorithms used to make determinations. Therefore, it becomes difficult to provide clear notice as to processing activities, as well as the means to opt out of such processing.
Body of Knowledge Domain I, Competency C

73. The correct answer is C. In a centralized data governance model, a central department manages and maintains the master copy of the data, sometimes referred to as the single source of truth. Other departments such as marketing that want to use the data make requests for specific data elements and those requests are handled by the central department. This ensures that the data is managed consistently but does not guarantee compliance or quick and easy access to the data.
Body of Knowledge Domain I, Competency A

74. The correct answer is D. Privacy liaisons or champions can act as departmental advocates for privacy initiatives and policies as well as identifiers of privacy risks, by integrating privacy representation in functional areas of an organization. Ron De Jesus, in "How to Operationalize Privacy by Design", contends that, "privacy champions should be identified across the company to act as force multipliers of the private messaging with their functional areas" (quoting Facebook Global Security Compliance and Privacy Head Kathy Del Gesso), and points out that, "[e]stablishing formal titles, like 'Privacy Champion' or 'Advocate' or 'Liaison,' is an effective way to garner interest among employees to volunteer for the added responsibilities".
Body of Knowledge Domain IV, Competency B

75. The correct answer is C. An audit is a tool to identify risks and gaps in procedural processes on an ongoing basis. It is critical to scope your audit to respond appropriately to the request.
Body of Knowledge Domain V, Competency B

76. The correct answer is C. The parent company is headquartered in Spain, part of the European Union, and it cannot transfer data freely to the affiliate company in Mexico without checks and balances as Mexico has not been deemed "adequate" by the European Commission. Therefore, according to Article 45, "There must be an adequate level of protection of personal data essentially equivalent to the protection of personal data in the European Union for data to freely travel from the European Union to another jurisdiction." In this case, the European Union and Mexico do not have this reciprocity and a standard contractual clause must be established.
Body of Knowledge Domain III, Competency C

77. The correct answer is A. While it is not required to provide a privacy notice when consent is the legal basis for processing, doing so allows customers to review and provide informed consent to the use of their personal data. The privacy notice should include all parties with whom data is shared; other parties would require the customer to provide information to them directly and should provide their own privacy notices. The other options are designed to promote different, yet sometimes broader, goals of how the company not only views privacy, but plans on executing those privacy views.
Body of Knowledge VI, Competency A

78. The correct answer is B. While it may be that there are other issues with how Marisol shared personal data, from the scenario it is clear that they did not obtain appropriate consent under the GDPR. Consent must be freely given, and be specific, informed and unambiguous. Jared was not asked to opt in for use of his personal data, he was not made aware of the parties with whom his information would be shared, nor was he told what specific information would be provided to them. Additionally, he did not consent to receive communications from these third parties.
Body of Knowledge VI, Competency A

79. The correct answer is C. The first action to take to stop the future materials from populating his inbox would be to unsubscribe from future contact. However, it is also important to carry out "spot checks" to ensure this link is operational. If the advertising/promotional emails continue, then the link may not work or the request was not

honored.
Body of Knowledge VI, Competency A

80. The correct answer is D. The data protection officer (DPO) is best suited to determine the frequency of the review, because they know the legal requirements, the nature of the business, the risks associated with the type, and volume of processing undertaken by the organization and the supervisory authority focus. These are all key components in the decision-making process regarding the frequency of the review.
Body of Knowledge Domain II, Competency B

81. The correct answer is A. Company B has fully documented and implemented procedures and processes. This phase indicates that the company could improve in measuring and refining its processes but has appropriate processes in place.
Body of Knowledge Domain III, Competency A

82. The correct answer is A. A given process, which may initially seem privacy intrusive, may be appropriate when combined with other measures that ensure all seven principles of privacy by design are met.
Body of Knowledge Domain IV, Competency B

83. The correct answer is A. Discussing the updates with the legal department and comparing the old and new policies will help determine what the changes are, but will not determine whether the existing privacy program complies with those changes. Audits of privacy programs should be done on a regular basis to ensure that any changes in technology or legal requirements are met. When a specific update or change occurs, an audit should be performed immediately to be certain that the organization continues to comply with all requirements, internal or external. Reactive response, i.e., waiting for a complaint, is never in an organization's best interest.
Body of Knowledge Domain V, Competency B

84. The correct answer is B. This question involves the data protection officer (DPO) requirements under the General Data Protection Regulation (GDPR). Article 37 of the GDPR establishes the specific criteria triggering the requirement for an organization to designate a DPO. The GDPR grants an exemption to courts and other independent judicial authorities from the requirement to appoint a DPO. Even if it is determined a DPO is not required, an organization may choose to voluntarily appoint one or multiple across different jurisdictions subject to this requirement. See GDPR, Recital 97 and GDPR, Article 37.
Body of Knowledge Domain I, Competency C

85. The correct answer is A. In the EU, data controllers determine how data will be processed and by whom. Even when data is shared for processing purposes, the controller—in this case, Company A—retains the control over all aspects of the data, including when and how processors delete it. To that end, OldPay would be required to delete the records according to the contract it has with Company A. In regions where there is no overarching data protection regulation, it is even more critical that contracts clearly specify how and when data is to be

deleted to protect personal data from accidental deletion or potential misuse.
Body of Knowledge Domain III, Competency B

86. The correct answer is C. Each of the other options have valid and important questions that must be considered in the development of an effective internal communications plan by the privacy program management team. However, the questions presented in the correct response will need to be established and answered *before* the privacy program management team and the communications team can have an effective relationship.
Body of Knowledge Domain IV, Competency A

87. The correct answer is D. Key risk indicators (KRIs) are an essential metrics tool that help a company predict risks that can unfavorably impact their business. Key performance indicators (KPIs) can be applied to people, processes and technologies that are critical to a business and assess progress against a company's declared goals and objectives, as well as measure and analyze trends in business performance. Confusion can occur when an organization uses the two terms interchangeably.
Body of Knowledge Domain II, Competency C

88. The correct answer is C. While terminology may differ between jurisdictions, generally, XCompany would be identified as a data controller. They determine how the data they provide can be processed and by whom. VendorZ would be considered one of their processors. Since XCompany retains control of the data, VendorZ must obtain their approval before hiring a sub-processor. In some jurisdictions, such as in the EU, this is required by law.
Body of Knowledge Domain III, Competency B

89. The correct answer is B. Privacy managers come from various backgrounds and levels of expertise. Many privacy managers have a legal background; however, other areas of expertise, such as auditing, information security, information technology, sector experience (e.g., healthcare), and/or project management can lend the experience and skills necessary to create successful privacy managers. The field of privacy management is dynamic and ever-changing. Therefore, regardless of one's background or training, successful privacy officers should have the skills necessary to adapt to the changes around them and continuously improve the program based on day-to-day successes and failures. Simultaneously, they must also incorporate legislative, regulatory, and business requirement changes into their program.
Body of Knowledge Domain I, Competency A

90. The correct answer is D. A procuring organization may have specific standards and processes for vendor selection. A prospective vendor should be evaluated against these standards through questionnaires, privacy impact assessments and other checklists.
Organizations should be able to monitor the vendor's activities to ensure it is complying with contractual obligations. Audit needs can sometimes be satisfied through periodic assessments or reports by independent trusted parties regarding the vendor's practices. Results may indicate improvement areas that may be fixed or identify higher-level risk that may limit the ability of that vendor to properly perform privacy protections.
Body of Knowledge Domain III, Competency B

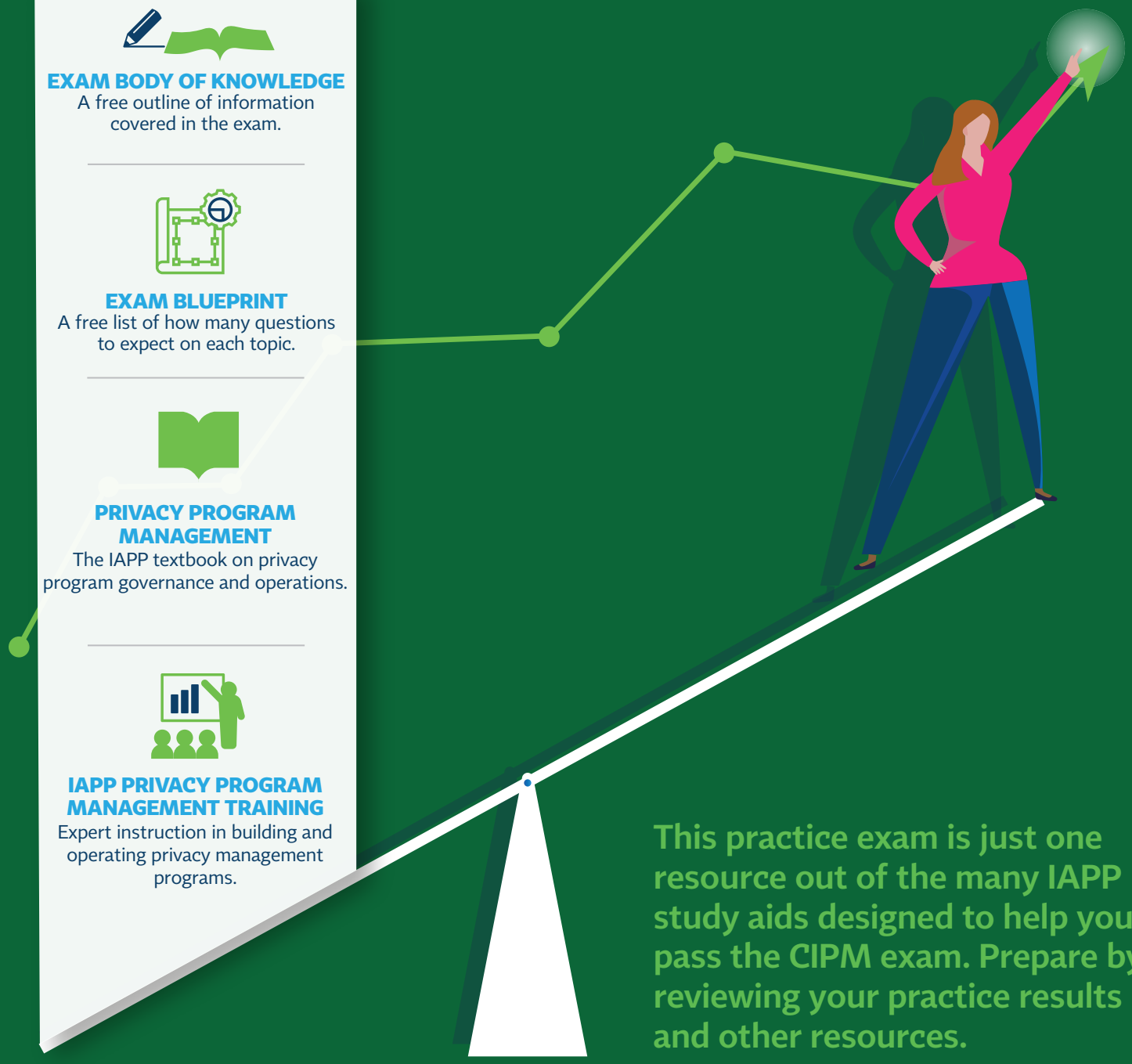
Build on Your Practice Exam Results

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.

PRIVACY PROGRAM MANAGEMENT
The IAPP textbook on privacy program governance and operations.

IAPP PRIVACY PROGRAM MANAGEMENT TRAINING
Expert instruction in building and operating privacy management programs.



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

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

Official IAPP Exam Preparation Resources