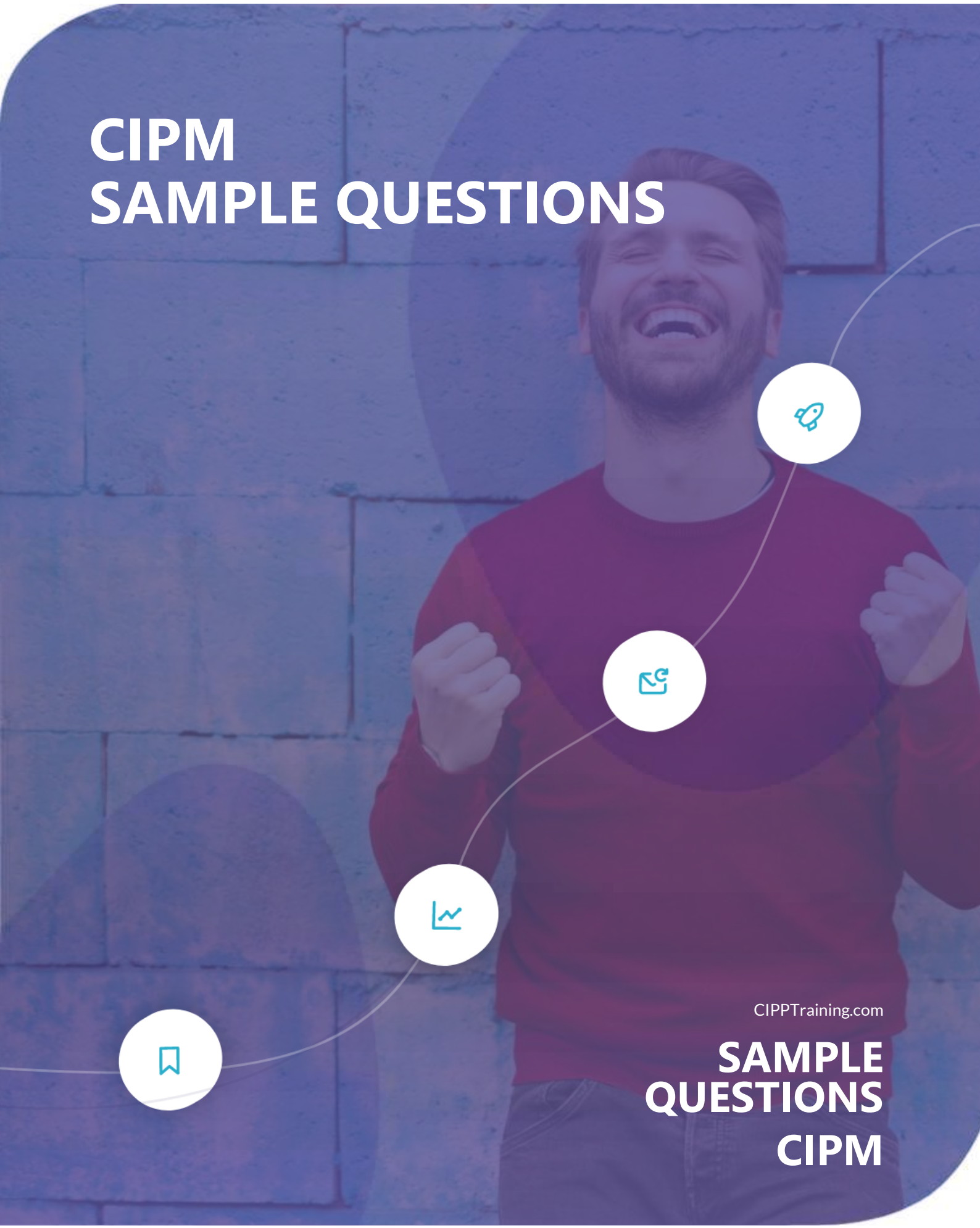
CIPM
SAMPLE QUESTIONS



CIPPTraining.com

SAMPLE QUESTIONS
CIPM

CIPM Sample Questions

Practice questions are indispensable for good exam preparation. Below you will find thirty IAPP style CIPM practice questions including two scenario questions.

The sample questions are part of our CIPM online training course. Our courses contain more than 300 of these practice questions. More information can be found at CIPPTraining.com.

1. All the following are responsibilities of a privacy program manager EXCEPT:

A. Identifying privacy obligations
B. Conducting program audits
C. Creating new procedures
D. Submit an annual report to the GDPR

2. Relating to Privacy Law, which term can best be defined as being able to prove that an organization is acting and demonstrating compliance with applicable laws?

A. Accountability
B. Privacy Governance
C. Privacy Framework
D. Data Map

3. Relating to Privacy Law, which term can best be defined as to guide a privacy function toward compliance with legal obligations and the organization's business objectives and goals?

A. Accountability
B. Privacy Governance
C. Privacy Framework
D. Data Map

4. Regarding privacy governance, which of the following describes where an organization stands on privacy?

A. The Scope of the Privacy Program
B. The Privacy Vision Statement
C. The Privacy Framework
D. The Privacy Strategy

5. In which component of privacy governance does an organization identify what personal information is processed and determine privacy obligations?

A. Selecting a Privacy Framework
B. Developing a Privacy Strategy
C. Defining Privacy Program Scope
D. Structuring the Privacy Team

6. Which component of privacy governance is defined as the organization's approach to communicating and obtaining support for the privacy program?

A. Selecting a Privacy Framework
B. Developing a Privacy Strategy
C. Defining Privacy Program Scope
D. Structuring the Privacy Team

7. During which component of Privacy Governance might a company gain buy-in to a new privacy program by conducting interviews and establishing program sponsors throughout the organization?

A. Selecting a Privacy Framework
B. Developing a Privacy Strategy
C. Defining Privacy Program Scope
D. Structuring the Privacy Team

8. Which privacy team model gives the most freedom of flexibility and a sense of ownership while allowing everyone to learn what works best for them, but it takes the most time to implement successfully?

A. Central
B. Hybrid
C. Local
D. Sectoral

9. Assuming that a candidate is qualified, which requirements must be met when appointing a Data Protection Officer?

A. They must have a privacy certification and 10 years' experience
B. They must be a line manager and integrated into the organization
C. They must have 5 years' experience as a privacy auditor
D. They must be independent and report to the highest level of the organization

Use the following scenario to answer questions 10-14.

Philip lives in the state of California and owns a gaming website. Most of his customers are between the age of 10 and 35. Philip is unfamiliar with privacy laws and wants to ensure that his business is compliant for operating in the US and especially California. A small number of customers live in the EU. Philip collects personal information for the purpose of directly marketing various games and accessories to his customers.

Philip has a privacy notice that he emails to new customers once they submit their email address at the start of membership sign-up. His notice contains information about his website, what information is processed, and how the data is used after collection.

Philip uses a popular credit card processing company for all his financial transactions and believes they are compliant regarding financial privacy laws so that he does not need to do anything additional to protect customers.

Philip needs a privacy professional to guide him through various California and other laws, so he understands his responsibilities regarding customer privacy on his website.

10. When explaining the Children's Online Privacy Protection Act to Philip, what age group does not need parent's permission to collect information, but Philip must obtain affirmative consent?:

A. 8 to 13 years old
B. 12 to 15 years old
C. 13 to 16 years old
D. 15 to 17 years old

11. Which California law must be explained to Philip that states he must have a legible privacy statement on his website?

A. California Online Privacy Protection Act
B. California Shine the Light Law
C. California Online Eraser Law
D. California Consumer Privacy Act

12. Philip will also need a process to receive and act upon requests from California customers to supply them with whatever information the company has collected about them, how it is used, and with whom it is disclosed and to opt-out of selling the information to third parties. Which California law can be cited to explain this to Philip?

A. California Online Privacy Protection Act
B. California Shine the Light Law
C. California Online Eraser Law
D. California Consumer Privacy Act

13. Dieter, a European citizen, has written an email to Philip. He stated he wanted his name to be modified in the database, because he recently had it changed, and asked for his postal address to be erased. Does Philip have to answer?

A. No, because he earlier gave full consent to the Philip
B. No, Philip would only have to if Dieter was an U.S. citizen
C. Yes, and even if it's a complex situation, Philip has to do it in under two months
D. Yes, and Philip normally has a month to do so

14. Philip decides to answer Dieter. Under the GDPR, should Philips change Dieter's name as requested?

A. Yes, and as controller he must ensure the data is modified appropriately
B. It's recommended that he does, but he is not under the legal obligation to do so
C. No, because Dieter gave full consent to use his old name
D. No, but Philip is obligated to add a note of the request to the database

15. Within privacy laws and regulations, which of the following is a voluntary code of conduct?

A. PCI DSS
B. HIPAA
C. FERPA
D. FRCA

16. Which of the following laws has the purpose of finding a balance between the free flow of data and the protection of the fundamental rights and freedoms of those to whom the data relates?

A. GDPR
B. HITECH
C. TCPA
D. COPPA

17. Which article of the GDPR defines the territorial scope of the GDPR?

A. Article 1
B. Article 3
C. Article 30
D. Article 65

18. All the following are TRUE concerning data assessments EXCEPT:

A. The Gramm-Leach-Bliley Act requires mandatory data mapping
B. The GDPR applies to both personal and non-personal data collection activities
C. Organizations with less than 250 employees that only collect data occasionally do not require a data inventory (processing records) under GDPR
D. Article 30 of GDPR contains reporting requirements for data processing activities

19. Which of the following data assessments is described as, "an analysis of the privacy risks associated with processing personal information in relation to a project, product, or service?"

A. Privacy Assessment
B. Privacy Impact Assessment
C. Second Party Audit
D. Comprehensive Data Mapping

20. Which privacy assessment describes a process designed to identify risks arising out of the processing of personal data and to minimize these risks as much and as early as possible. This assessment also has specific requirements outlined in Article 35 of the GDPR.

A. Privacy Assessment
B. Privacy Impact Assessment
C. Data Protection Impact Assessment
D. Comprehensive Data Mapping

21. Which type of data assessment must be completed according to the European Data Protection Board when evaluating or scoring an individual to determine his or her economic situation?

A. Privacy Assessment
B. Privacy Impact Assessment
C. Data Protection Impact Assessment
D. Comprehensive Data Mapping

22. Information Security is about preserving and protecting information regarding:

A. Availability
B. Integrity
C. Confidentiality
D. All the above

23. All the following statements are TRUE regarding data processing vendors and vendor selection EXCEPT:

A. Privacy risks on the part of the vendor must be exposed and remedied
B. Privacy responsibilities must be clearly documented in the contract
C. Vendors must help the primary company report any data breaches
D. The controller can only act on the instructions of the processor

24. Which elements should be included in an organizations privacy policy?

A. Purpose, Scope, Risk and Responsibilities, and Compliance Reasons
B. Scope, Framework, Strategy, and Team Structure
C. Purpose, Strategy, Scope, and Risk Assessment
D. Purpose, Scope, Strategy, and Team Structure

25. All the following statements regarding privacy policies are true, EXCEPT:

A. A privacy policy is a living document that adapts over time based on organizational needs
B. Specific guidelines and procedures are an elaboration of the privacy policy
C. A privacy policy is for external communication about the retention of personal data
D. A privacy committee may exist to communicate the privacy policy through an organization

Use the following scenario to answer questions 26-30.

Maria is the new Data Protect Officer at her company. The DPO is also the privacy team leader. Maria has been given new business objectives that the company is focusing on for the next year. Maria wants to map each business objective to the existing reports produced throughout the company so she can see if there are gaps requiring new reports.

Maria also wants to check the reverse and determine if the teams are developing reports that are no longer tied to business objectives. There have been some recent issues of management making business decisions based on the available metrics when it is clear the managers making the decision did not fully understand the limitations of the metric.

Lastly, the company will have an external auditor at the end of the year for recertification. The audit is extremely important since nearly all the company's biggest clients require TQM or ISO certification to be eligible to bid on projects.

26. Which of the following is an objective unit of measurement and must aligned with the company's business objectives?

A. SMART Goal
B. Enabling Objective
C. Performance Metric
D. Program Target

27. Which statement is true regarding the use of privacy metrics within the company?

A. Privacy metrics promote awareness to the importance of a business objective
B. Each privacy metric should be defined so everyone understands what the measurement indicates
C. Privacy metrics must be adaptable to the changing needs of the organization
D. All the statements above are true

28. Which type of data reporting may include measuring how long data is not available, such as in a disaster situation?

A. Return on Investment
B. Business Resiliency
C. Trend Analysis
D. Cataclysm Analysis

29. Regarding program maturity and tracking privacy compliance, at which level is data reporting first mapped out and specified?

A. Ad Hoc
B. Defined
C. Managed
D. Repeatable

30. What is the correct order of privacy audit phases, and what type of audit would be conducted by ISO or NIST?

A. A first party audit consisting of: Plan, Prepare, Audit, Report, and Follow-up
B. A second party audit consisting of: Prepare, Audit, Report, Plan Response, Follow-up
C. A third-party audit consisting of: Plan, Prepare, Audit, Report and Follow-up
D. A third-party audit consisting of: Plan, Prepare, Audi, Follow-up, Formal Report

References

1. Answer: D. The GDPR does not required an annual report.

2. Answer: A. Accountability is a major concept in new data protection laws.

3. Answer: B. Privacy governance is required for building a strong privacy program.

4. Answer: B. The privacy vision or mission statement describes where the organization stands regarding privacy in just a few sentences.

5. Answer: C. While defining the scope of the privacy program an organization should identify what personal information is to be processed and then identify privacy obligations related to the data collected.

6. Answer: B. Developing a privacy strategy is completed after the vision statement has been written, and both scope and framework have been determined.

7. Answer: B. Conducting privacy workshops and assisting with ongoing projects to investigate privacy requirements jointly may also be done.

8. Answer: B. The central model is quick and easy but tends to exclude rather than include. Most companies use a hybrid that combines both the central and local model.

9. Answer: Answer: D. DPO's are appointed voluntarily, but they must be independent and report to the highest level of management to remain objective and free of organizational influences.

10. Answer: C. Under the age of 13 requires a parent's consent. 13 to 16 years of age can give consent, but it must be affirmed, such as clicking on a box.

11. Answer: A. CalOPPA states that websites that collect personal information from California consumers are required to place a privacy notice on their website.

12. Answer: D. The California Consumer Protect Act provides for these rights of consumers.

13. Answer: D. Article 12 (3) GDPR stipulates that the controller (Philip) has a month to comply with the requests of data subjects. Starting with the receipt of the request. This period can be extended by two months in specific situations and/or in case of complex applications.

14. Answer: A. See Article 16 GDPR. The controller must ensure the data is modified appropriately.

15. Answer: A. The payment card industry data security standard for protecting credit card data is likely the best-known voluntary code of conduct within a large industry.

16. Answer: A. The GDPR provides general protections and regulations to find the balance between the free flow of data and the protection of the fundamental rights and freedoms of those to whom the data applies.

17. Answer: B. Article 3 defines the territorial scope of the GDPR.

18. Answer: B. GDPR only applies to personal data.

19. Answer: B. The PIA, which must also include measures to reduce the identified risks.

20. Answer: C. The DPIA and PIA basically require the same thing, but DPIA has specific requirements under the GDPR.

21. Answer: C. The EDPB requires that a DPIA be conducted in this situation.

22. Answer: D. CIA = Confidentiality, Integrity, and Availability

23. Answer: D. Vendors (processors) must follow the directions of the controller, or risk becoming subject to the additional laws and obligations of being a controller.

24. Answer: A. It is specifically recommended that a privacy policy include the purpose, scope, risk and responsibilities, and compliance reasons.

25. Answer: C. A privacy policy is for internal communication whereas a privacy note is for external communication.

26. Answer: C. Every performance metric should have an owner who is responsible for the underlying processes that move the metric.

27. Answer: D. Metrics are not easy. Identifying and identifying exactly which metrics are important and reflect the business objects are always intuitive.

28. Answer: B. Business resiliency metrics refer to how well the business withstands crisis.

29. Answer: B. Level 3 is Defined. It is not yet regularly reviewed, nor does it have continuous improvement efforts.

30. Answer: C. ISO and NIST are forms of third-party audit that are usually lengthy and result in certification, or re-certification. Neither ISO nor NIST can determine if your processes or systems are good. They can only determine that you have a documented process, follow that process, and have continuous improvement efforts in place.