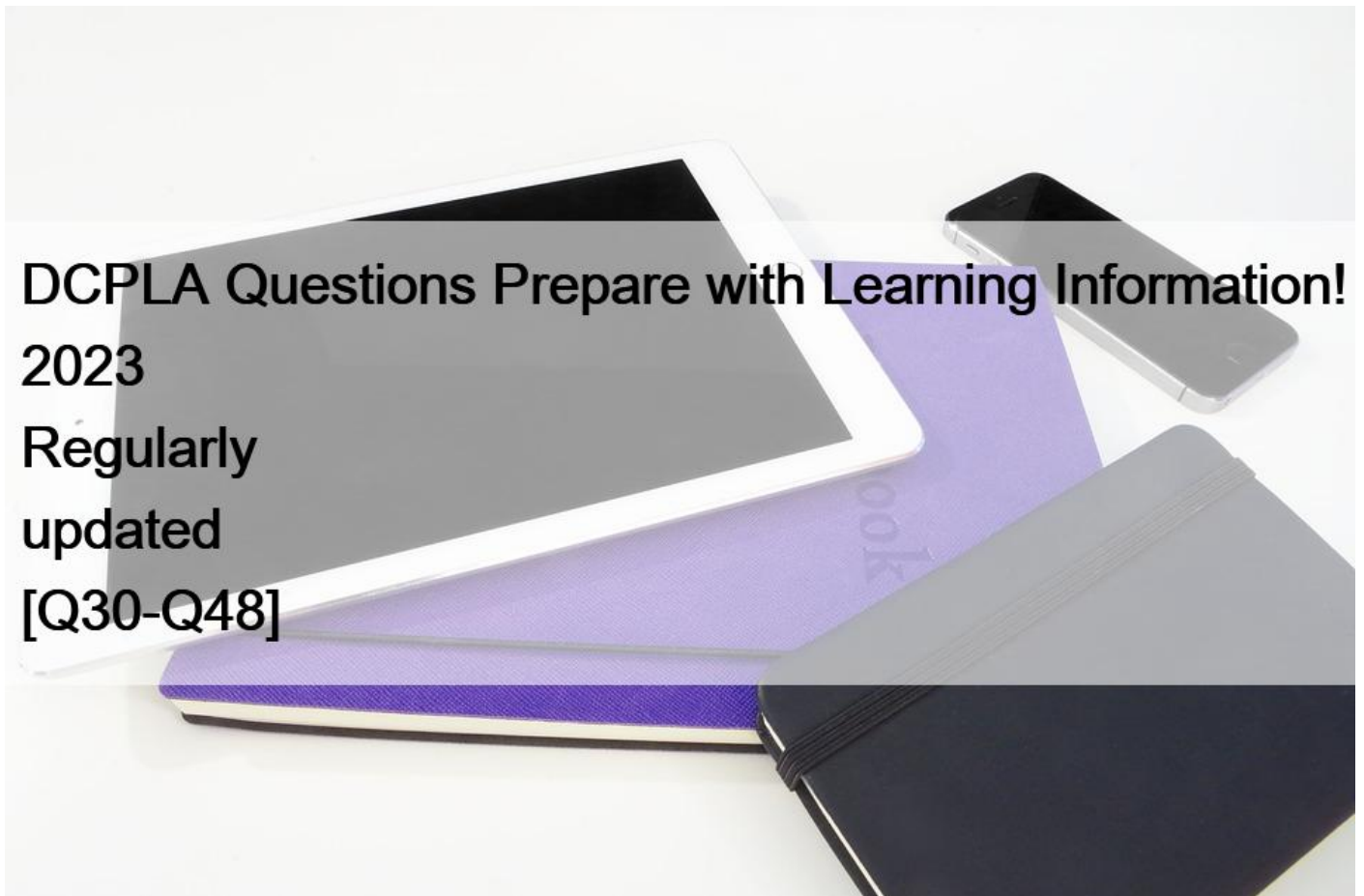


DCPLA Questions Prepare with Learning Information! 2023 Regularly updated [Q30-Q48]



DCPLA Questions Prepare with Learning Information! 2023 Regularly updated
Get DCPLA Products Practice Material for DCPLA Exam Question Preparation

DSCI Certified Privacy Lead Assessor DCPLA certification exam is a comprehensive and rigorous exam that tests the candidate's knowledge and skills in privacy management and assessment. DSCI Certified Privacy Lead Assessor DCPLA certification is recognized globally and is ideal for professionals who want to enhance their career prospects in the field of data protection and privacy. DSCI Certified Privacy Lead Assessor DCPLA certification is offered by the Data Security Council of India, a leading organization that works towards enhancing data protection and privacy in India.

NEW QUESTION 30

FILL BLANK

IUA and PAT

The company has a very mature enterprise level access control policy to restrict access to information. There is a single sign-on platform available to access company resources such as email, intranet, servers, etc. However, the access policy in client relationships varies depending on the client requirements. In fact, in many cases clients provide access ids to the employees of the company and manage them. Some clients also put technical controls to limit access to information such data masking tool, encryption, and anonymizing data, among others. Some clients also record the data collection process to monitor if the employee of the company does not collect more data than is required. Taking cue from the best practices implemented by the clients, the company, through the consultants, thought of realigning its access control policy to include control on data collection and data usage by the business functions and associated third parties. As a first step, the consultants advised the company to start monitoring the PI collection, usage and access by business functions without their knowledge. The IT function was given the responsibility to do the monitoring, as majority of the information was handled electronically. The analysis showed that many times, more information than necessary was collected by the some functions, however, no instances of misuse could be identified.

After few days of this exercise, a complaint was registered by a female company employee in the HR function against a male employee in IT support function. The female employee accused the male employee of accessing her photographs stored on a shared drive and posting it on a social networking site.

(Note: Candidates are requested to make and state assumptions wherever appropriate to reach a definitive conclusion) Introduction and Background XYZ is a major India based IT and Business Process Management (BPM) service provider listed at BSE and NSE. It has more than 1.5 lakh employees operating in 100 offices across 30 countries. It serves more than 500 clients across industry verticals – BFSI, Retail, Government, Healthcare, Telecom among others in Americas, Europe, Asia-Pacific, Middle East and Africa. The company provides IT services including application development and maintenance, IT Infrastructure management, consulting, among others. It also offers IT products mainly for its BFSI customers.

The company is witnessing phenomenal growth in the BPM services over last few years including Finance & Accounting including credit card processing, Payroll processing, Customer support, Legal Process Outsourcing, among others and has rolled out platform based services. Most of the company's revenue comes from the US from the BFSI sector. In order to diversify its portfolio, the company is looking to expand its operations in Europe. India, too has attracted company's attention given the phenomenal increase in domestic IT spend esp. by the government through various large scale IT projects. The company is also very aggressive in the cloud and mobility space, with a strong focus on delivery of cloud services. When it comes to expanding operations in Europe, company is facing difficulties in realizing the full potential of the market because of privacy related concerns of the clients arising from the stringent regulatory requirements based on EU General Data Protection Regulation (EU GDPR).

To get better access to this market, the company decided to invest in privacy, so that it is able to provide increased assurance to potential clients in the EU and this will also benefit its US operations because privacy concerns are also on rise in the US. It will also help company leverage outsourcing opportunities in the Healthcare sector in the US which would involve protection of sensitive medical records of the US citizens.

The company believes that privacy will also be a key differentiator in the cloud business going forward. In short, privacy was taken up as a strategic initiative in the company in early 2011.

Since XYZ had an internal consulting arm, it assigned the responsibility of designing and implementing an enterprise wide privacy program to the consulting arm. The consulting arm had very good expertise in information security consulting but had limited expertise in the privacy domain. The project was to be driven by CIO's office, in close consultation with the Corporate Information Security and Legal functions.

What role can training and awareness play here? (250 to 500 words)

Training and awareness play an essential role in the successful implementation of a comprehensive privacy program. This is especially true for an organization that has limited expertise on the subject. Training and awareness help to ensure that everyone understands their obligations under the EU GDPR as well as other applicable laws and regulations, while also providing employees with best practices to ensure data protection.

One way to ensure optimal training and awareness is by creating a comprehensive training curriculum tailored specifically for XYZ's needs. The curriculum should cover topics such as data privacy rights, compliance requirements, impact assessment, access control measures, encryption technologies, incident response plans and more. Additionally, it should be augmented with practical examples so that employees can understand how these principles apply in different scenarios.

Moreover, a comprehensive awareness program should be established to keep all employees informed of the latest developments in privacy law. This can include newsletters, webinars and other communications that explain changes in laws or policies, provide information on new technologies, or even give advice on how to handle particular challenges.

Finally, management should ensure that there are measures in place to evaluate the effectiveness of the training and awareness programs. This can include surveys, interviews with staff members and other methods such as focus groups or workshops. All these means will help XYZ assess whether its employees understand their obligations under the GDPR and other applicable laws and regulations.

By creating a comprehensive training curriculum tailored specifically for its needs and establishing an effective awareness program, XYZ can ensure that everyone in the organization is better informed and aware of their responsibilities under the GDPR. This, in turn, will help to improve compliance with the applicable laws and regulations while protecting its customers' data. Ultimately, this will allow the company to realize its full potential on the European market.

By investing in training and awareness programs, XYZ demonstrates a commitment to proper privacy procedures which will not only benefit its operations in Europe but also those in the US. It is essential for any company operating today to prioritize privacy so that it can build client trust as well as remain compliant with regulations. With an effective training and awareness program in place, XYZ can confidently approach both current and potential clients knowing that their data will be secure.

Overall, training and awareness are important components of a successful privacy program. By investing in these programs, XYZ can ensure that everyone is informed and aware of their responsibilities under the GDPR and other applicable laws and regulations. This, in turn, will help to protect customer data while also improving compliance with applicable laws. Ultimately, this will help XYZ realize its full potential on the European market as well as build client trust.

By establishing a comprehensive training and awareness program, XYZ will be better prepared to handle the challenges of data privacy regulation. With the proper methods in place, the company can not only protect its customers' data but also remain compliant with laws and regulations. This, in turn, will help it achieve success on both domestic and international markets. Ultimately, investing in training and awareness is essential for any organization operating today.

NEW QUESTION 31

Which of the following is not an objective of POR?

- * Create an inventory of business processes, enterprise and operational functions, client relationships that deal with personal information
- * Identify all the activities, functions and operations that can be attributed to the privacy initiatives of an organization
- * Evaluate the role of corporate function in legal compliance management, its relations with IT, and security functions. Evaluate the role of legal function in compliance matters
- * Establish a privacy function to address the activities, functions and operations that are required to manage the privacy initiatives

NEW QUESTION 32

Following aspects can serve as inputs to a privacy organization for ensuring privacy protection:

- I) Privacy related incidents detected/reported

II) Contractual obligations

III) Organization's exposure to personal information

IV) Regulatory requirements

- * I, II and III
- * II and IV
- * I, II, III and IV
- * None of the above, as privacy and compliance protection mechanisms are evolved based only on organization's privacy policies and procedures

NEW QUESTION 33

An organization is always a data controller for its _____.

- * Employees
- * Client
- * Supervisory authority
- * None of the above

NEW QUESTION 34

Which of the following is not an objective of VPI?

- * To enable identification of processes, functions and relationships handling personal information
- * Assess the current state of data spread and transactions of the organization to map this against its privacy objectives
- * Enable an organization to map its data operations and categorization of PI
- * None of the above

NEW QUESTION 35

As a privacy assessor, what would most likely be the first artefact you would ask for while assessing an organization which claims that it has implemented a privacy program?

- * Privacy risk management framework
- * Records of privacy specific training imparted to the employees handling personal information
- * Personal information management policy
- * Records of deployed privacy notices and statements

NEW QUESTION 36

FILL BLANK

PPP

Based on the visibility exercise, the consultants created a single privacy policy applicable to all the client relationships and business functions. The policy detailed out what PI company deals with, how it is used, what security measures are deployed for protection, to whom it is shared, etc. Given the need to address all the client relationships and business functions, through a single policy, the privacy policy became very lengthy and complex. The privacy policy was published on company's intranet and also circulated to heads of all the relationships and functions. W.r.t. some client relationships, there was also confusion whether the privacy policy should be notified to the end customers of the clients as the company was directly collecting PI as part of the delivery of BPM services. The heads found it difficult to understand the policy (as they could not directly relate to it) and what actions they

need to perform. To assuage their concerns, a training workshop was conducted for 1 day. All the relationship and function heads attended the training.

However, the training could not be completed in the given time, as there were numerous questions from the audiences and it took lot of time to clarify.

(Note: Candidates are requested to make and state assumptions wherever appropriate to reach a definitive conclusion) Introduction and Background XYZ is a major India based IT and Business Process Management (BPM) service provider listed at BSE and NSE. It has more than 1.5 lakh employees operating in 100 offices across 30 countries. It serves more than 500 clients across industry verticals – BFSI, Retail, Government, Healthcare, Telecom among others in Americas, Europe, Asia-Pacific, Middle East and Africa. The company provides IT services including application development and maintenance, IT Infrastructure management, consulting, among others. It also offers IT products mainly for its BFSI customers.

The company is witnessing phenomenal growth in the BPM services over last few years including Finance & Accounting including credit card processing, Payroll processing, Customer support, Legal Process Outsourcing, among others and has rolled out platform based services. Most of the company's revenue comes from the US from the BFSI sector. In order to diversify its portfolio, the company is looking to expand its operations in Europe. India, too has attracted company's attention given the phenomenal increase in domestic IT spend esp. by the government through various large scale IT projects. The company is also very aggressive in the cloud and mobility space, with a strong focus on delivery of cloud services. When it comes to expanding operations in Europe, company is facing difficulties in realizing the full potential of the market because of privacy related concerns of the clients arising from the stringent regulatory requirements based on EU General Data Protection Regulation (EU GDPR).

To get better access to this market, the company decided to invest in privacy, so that it is able to provide increased assurance to potential clients in the EU and this will also benefit its US operations because privacy concerns are also on rise in the US. It will also help company leverage outsourcing opportunities in the Healthcare sector in the US which would involve protection of sensitive medical records of the US citizens.

The company believes that privacy will also be a key differentiator in the cloud business going forward. In short, privacy was taken up as a strategic initiative in the company in early 2011.

Since XYZ had an internal consulting arm, it assigned the responsibility of designing and implementing an enterprise wide privacy program to the consulting arm. The consulting arm had very good expertise in information security consulting but had limited expertise in the privacy domain. The project was to be driven by CIO's office, in close consultation with the Corporate Information Security and Legal functions.

Do you agree with company's decision to have single privacy policy for all the relationships and functions?

Please justify your view. (250 to 500 words)

Explanation

Yes, I agree with the company's decision to have a single privacy policy for all its relationships and functions.

Having a unified privacy policy allows the organization to communicate consistently across multiple channels of communication with customers, partners and vendors. It also ensures that all stakeholders are aware of their rights when dealing with personal data and makes it easier for them to understand their responsibilities when handling such information.

Moreover, having a standardized privacy policy helps to protect the company from potential legal repercussions due to inadequate protection of confidential data. The need for comprehensive protection is especially important in this age where cyber-attacks are becoming increasingly frequent and sophisticated. By putting in place a consistent framework that governs how any organization handles sensitive information can help reduce the risks associated with data breaches.

By demonstrating that the company takes strong measures to protect its customers' personal information, a single privacy policy can help boost the company's reputation and build trust with customers. Compliance with a variety of regulatory requirements is especially important for companies operating in regulated industries, such as banking and healthcare.

In addition, having a unified privacy policy allows organizations to maintain control over how their data is stored and processed. By monitoring who has access to confidential information, companies can identify any potential security vulnerabilities before they are exploited by malicious actors.

To conclude, I support XYZ's decision to have one privacy policy for all its relationships and functions.

Having a unified privacy policy can help the organization protect itself from potential legal risks, boost its reputation and maintain control over how data is stored and used. All in all, it is an important step to ensure that customer data is always kept safe and secure.

NEW QUESTION 37

Create an inventory of the specific contractual terms that explicitly mention the data protection requirements.

This an imperative of which DPF practice area?

- * Visibility over Personal Information (VPI)
- * Information Usage and Access (IUA)
- * Privacy Contract Management (PCM)
- * Regulatory Compliance Intelligence (RCI)

NEW QUESTION 38

Map the legal and compliance requirements to each data element that an organization is dealing with in all of its business processes, enterprise and operational functions, and client relationships. This an imperative of which DPF practice area?

- * Visibility over Personal Information (VPI)
- * Privacy Organization and Relationship (POR)
- * Regulatory Compliance Intelligence (RCI)
- * Privacy Policy and Processes (PPP)

NEW QUESTION 39

Which of the following are key contributors that would enhance the complexity in implementing security measures for protection of personal information? (Choose all that apply.)

- * Data collection through multiple modes and channels
- * Evolution of nimble and flexible business processes affecting access management
- * Regulatory requirements to issue privacy notice and data breach notification in specified format
- * None of the above

NEW QUESTION 40

Categorize the following statements as: Visibility/ Capability /Enforcement /Demonstration Problems

The network is unable to restrict unwanted external connections carrying sensitive information.

- * Visibility
- * Capability

- * Enforcement
- * Demonstration

NEW QUESTION 41

FILL BLANK

RCI and PCM

Given its global operations, the company is exposed to multiple regulations (privacy related) across the globe and needs to comply mostly through contracts for client relationships and directly for business functions. The corporate legal team is responsible for managing the contracts and understanding, interpreting and translating the legal requirements. There is no formal tracking of regulations done. The knowledge about regulations mainly comes through interaction with the client team. In most of the contracts, the clients have simply referred to the applicable legislations without going any further in terms of their applicability and impact on the company. Since business expansion is the priority, the contracts have been signed by the company without fully understanding their applicability and impact. Incidentally, when the privacy initiatives were being rolled out, a major data breach occurred at one of the healthcare clients located in the US. The US state data protection legislation required the client to notify the data breach. During investigations, it emerged that the data breach happened because of some vulnerability in the system owned by the client but managed by the company and the breach actually happened 5 months back and came to notice now. The system was used to maintain medical records of the patients. This vulnerability had been earlier identified by a third party vulnerability assessment of the system and the closure of vulnerability was assigned to the company. The company had made the requisite changes and informed the client. The client, however, was of the view that the changes were actually not made by the company and they therefore violated the terms of contract which stated that "the company shall deploy appropriate organizational and technology measures for protection of personal information in compliance with the XX state data protection legislation." The company could not produce necessary evidences to prove that the configuration changes were actually made by it (including when these were made).

(Note: Candidates are requested to make and state assumptions wherever appropriate to reach a definitive conclusion) Introduction and Background XYZ is a major India based IT and Business Process Management (BPM) service provider listed at BSE and NSE. It has more than 1.5 lakh employees operating in 100 offices across 30 countries. It serves more than 500 clients across industry verticals BFSI, Retail, Government, Healthcare, Telecom among others in Americas, Europe, Asia-Pacific, Middle East and Africa. The company provides IT services including application development and maintenance, IT Infrastructure management, consulting, among others. It also offers IT products mainly for its BFSI customers.

The company is witnessing phenomenal growth in the BPM services over last few years including Finance & Accounting including credit card processing, Payroll processing, Customer support, Legal Process Outsourcing, among others and has rolled out platform based services. Most of the company's revenue comes from the US from the BFSI sector. In order to diversify its portfolio, the company is looking to expand its operations in Europe. India, too has attracted company's attention given the phenomenal increase in domestic IT spend esp. by the government through various large scale IT projects. The company is also very aggressive in the cloud and mobility space, with a strong focus on delivery of cloud services. When it comes to expanding operations in Europe, company is facing difficulties in realizing the full potential of the market because of privacy related concerns of the clients arising from the stringent regulatory requirements based on EU General Data Protection Regulation (EU GDPR).

To get better access to this market, the company decided to invest in privacy, so that it is able to provide increased assurance to potential clients in the EU and this will also benefit its US operations because privacy concerns are also on rise in the US. It will also help company leverage outsourcing opportunities in the Healthcare sector in the US which would involve protection of sensitive medical records of the US citizens.

The company believes that privacy will also be a key differentiator in the cloud business going forward. In short, privacy was taken up as a strategic initiative in the company in early 2011.

Since XYZ had an internal consulting arm, it assigned the responsibility of designing and implementing an enterprise wide privacy program to the consulting arm. The consulting arm had very good expertise in information security consulting but had limited expertise in the privacy domain. The project was to be driven by CIO's office, in close consultation with the Corporate Information Security and Legal functions.

Why do you think the company failed to defend itself against client accusations? (250 to 500 words)

The company failed to defend itself against accusations by its clients most likely due to the fact that it did not have enough expertise in privacy and data protection. The company's privacy program was designed and implemented by an internal consulting arm which had limited expertise in the domain, causing the program to be inadequate for the purpose of defending itself against accusations. Moreover, since the project was driven by CIO's office, there may have been a lack of coordination between different functions like Corporate Information Security and Legal functions which could also have contributed to the failure.

It is possible that there were gaps in the organizational measures deployed by XYZ as well as gaps in technology measures. For example, it is possible that although appropriate organizational measures were put in place, the technology measures were inadequate for protecting the sensitive data of its clients. In addition, it is possible that the company did not rigorously monitor compliance with these organizational and technological measures, thereby making it vulnerable to accusations by its clients.

It is also likely that XYZ was unable to fully comply with applicable privacy laws and regulations in the EU due to lack of awareness about their requirements as well as insufficient resources allocated for adapting to them. The EU GDPR requires companies to implement appropriate technical and organizational measures for the protection of personal data which could have been a challenge for XYZ given its limited expertise in this domain. Furthermore, even though it may have had some understanding of the legal requirements, there may have been difficulty in properly implementing them, which could have led to the accusations by its clients.

Finally, it is possible that XYZ failed to defend itself against client accusations because of a lack of communication between its different departments and functions. The company may not have had a clear understanding of the requirements and risks associated with data protection and privacy compliance which could have caused miscommunication among various stakeholders leading to inadequate responses when it was challenged by its clients.

Overall this case study demonstrates the importance of properly designing and implementing an effective privacy program in order to protect sensitive data from unauthorized access or misuse. Companies should ensure that they have adequate expertise in data protection as well as sufficient resources for adapting to changing regulatory requirements in order to avoid potential legal issues arising from client accusations.

Effective communication and coordination across different departments and functions is also essential for successful data protection compliance.

It is recommended that companies invest in an ongoing training program to ensure that employees understand the importance of privacy, have an awareness of the legal requirements, and are able to properly implement security measures to protect sensitive data. Organizations should also consider implementing automated tools and technologies such as encryption, access control systems, identity management solutions, etc., which can help them better defend themselves against potential client accusations.

NEW QUESTION 42

An entity shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed; or with respect to an established retention period. This privacy principle is known as?

- * Collection Limitation
- * Use Limitation
- * Security safeguards

- * Storage Limitation

NEW QUESTION 43

“Data which cannot be attributed to a particular data subject without use of additional information.” Which of the following best describes the above statement?

- * Anonymized Data
- * Metadata
- * Pseudonymized Data
- * None of the above

NEW QUESTION 44

Section 43A of the Information Technology (Amendment) Act, 2008 holds _____ accountable for having reasonable security practices and procedures in place to protect sensitive personal data.

- * Government
- * Body corporates
- * Government and body corporates alike
- * None of the above

NEW QUESTION 45

What are the two phases of DSCI Privacy Third Party Assessment?

- * Initial and Detailed
- * Primary and Secondary
- * Initial and Final
- * None of the above

NEW QUESTION 46

Which of the following mechanisms can be used to transfer personal data outside of a country?

- * Binding corporate rules
- * Adequacy decision
- * Standard contractual clauses
- * All of the above

NEW QUESTION 47

Which of the following are the key factors that need to be considered for determining the applicability of the privacy principles? (Choose all that apply.)

- * The role of the organization in determining the purpose of the data collection
- * How and where the data is coming in the organization
- * Requirements stipulated by the local authorities from where the organization is operating
- * Organization's commitment to the external stakeholder with respect to privacy

NEW QUESTION 48

A newly appointed Data Protection officer is reviewing the organization's existing privacy policy. Which of the following would be the most critical factor for the review process?

- * Awareness of the business units about the privacy policy

- * Changes in the legal/regulatory regime
- * Privacy policies of industry peers
- * Foreseeable challenges in the effective implementation of the policy

The DCPLA certification exam covers a wide range of topics, including privacy laws and regulations, risk assessment and management, data protection strategies, and privacy impact assessment. DCPLA exam is designed to assess an individual's ability to evaluate and manage privacy risks, as well as their knowledge of best practices in privacy management. DCPLA exam is rigorous and requires extensive preparation and study to pass.

Most Reliable DSCI DCPLA Training Materials: <https://www.validbraindumps.com/DCPLA-exam-prep.html>