

DCPLA Latest Exam Forum, DCPLA Test Labs



P.S. Free 2025 DSCI DCPLA dumps are available on Google Drive shared by PDF4Test: <https://drive.google.com/open?id=1-sjNYKF8kAu8a6pLcGecVTiosDaqK3t>

People who get DCPLA certification show dedication and willingness to work hard, also can get more opportunities in job hunting. It seems that DCPLA certification becomes one important certification for many IT candidates. While a good study material will do great help in DCPLA Exam Preparation. PDF4Test DCPLA will solve your problem and bring light for you. DCPLA exam questions and answers are the best valid with high hit rate, which is the best learning guide for your DSCI DCPLA preparation.

The DCPLA certification exam is a globally recognized certification that is highly valued by employers and organizations across various industries. DSCI Certified Privacy Lead Assessor DCPLA certification program is designed to provide individuals with comprehensive knowledge and skills to assess and manage privacy risks in organizations. DSCI Certified Privacy Lead Assessor DCPLA Certification exam is an excellent opportunity for professionals who are looking to enhance their career prospects in the field of privacy assessment and management. Furthermore, the certification program is an excellent way to demonstrate one's commitment to privacy and data protection practices, which is becoming increasingly important in today's digital world.

>> DCPLA Latest Exam Forum <<

[2026] DSCI DCPLA Questions: Fosters Your Exam Passing Skills

IT industry is growing very rapidly in the past few years, so a lot of people start to learn IT knowledge, so that keep them for future success efforts. DSCI DCPLA certification exam is essential certification of the IT industry, many people frustrated by this certification. Today, I will tell you a good way to pass the exam which is to choose PDF4Test DSCI DCPLA Exam Training materials. It can help you to pass the exam, and we can guarantee 100% pass rate. If you do not pass, we will guarantee to refund the full purchase cost. So you will have no losses.

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.

DSCI Certified Privacy Lead Assessor DCPLA certification Sample Questions (Q19-Q24):

NEW QUESTION # 19

XYZ bank has recently decided to start offering online banking services. For doing so, the bank has outsourced its IT operations and processes to various third parties. Acknowledging privacy concerns, bank has decided to implement a privacy program. Assuming you have been tasked to deploy this framework for the bank, which of the following would most likely be your first step?

- A. None of the above

- B. Create an inventory of business processes that deal with personal information and identify the associated data element
- C. Assign privacy roles and responsibilities for process owners
- D. Ensure that bank is equipped to test the relevance of each legal and compliance requirement in its environment

Answer: B

Explanation:

Under the "Visibility over Personal Information (VPI)" practice area of the DSCI Privacy Framework, the first and foundational step in any privacy implementation is to:

"Create an inventory of business processes and associated data elements involving personal information." This baseline mapping ensures that organizations understand what data is processed, where it resides, and how it flows across systems and third parties. This forms the basis for subsequent governance, risk assessment, and compliance alignment.

NEW QUESTION # 20

FILL BLANK

RCI and PCM

In April 2011, the rules were issued under Section 43A of the IT Act by the Government of India and the 'body corporates' were required to comply with these rules. The Corporate legal team tried to understand and interpret the rules but struggled to understand its applicability esp. to client relationships and business functions. So, the company hired an IT Act legal expert to advise them on the Section 43A rules.

To start with, the company identified the PI dealt with by business functions as part of the earlier visibility exercise, but it wanted to reassure itself. Therefore, a specific exercise was conducted to revisit 'sensitive personal information' dealt with by business functions. It was realized that the company collects lot of SPI of its employees and therefore 'reasonable security practices' need to be adhered to by the functions that deal with SPI. It was also ascertained that many of this SPI is being dealt by third parties, some of which are also located outside India. To meet the requirements of the rules, the company reviewed all the contracts and inserted a clause - 'the service provider shall implement reasonable security practices and procedures as per the IT (Amendment) Act, 2008'. Some of the large service providers were ISO 27001 certified and they claimed that they fulfill the requirements of 'reasonable security practices'. However, some SME service providers did not understand what would 'reasonable security practices' imply and requested the company to clarify, which referred them to Rule 8 of the Section 43A. Some small scale service providers expressed their unwillingness to get ISO certified, given the costs involved.

(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 and 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.

Did the company take sufficient steps to protect SPI dealt by its service providers and ensure that it complies with the regulatory requirements? Was referring to 'reasonable security practices' sufficient in the contracts or the company should have also considered some other measures for privacy protection as well? (250 to 500 words)

Answer:

Explanation:

See the answer in explanation below.

Explanation:

The consulting arm of XYZ developed a comprehensive privacy program in line with the company's goal to leverage its existing technology infrastructure, resources and capabilities for protecting data. The program had three parts - awareness and training, policy development and implementation. On the awareness front, extensive training was conducted for employees on various aspects of privacy including GDPR compliance.

This was followed by the development and rollout of an enterprise-wide privacy policy which clearly defined the various steps to be taken to protect sensitive personal information (SPI) such as encryption, access controls etc. After this, customer contracts were reviewed for appropriate protection clauses and service providers were made to sign 'reasonable security practices' clauses in their contractual obligations as specified in EU GDPR.

At first glance, it seemed that XYZ had taken adequate steps to protect SPI dealt by its service providers and ensure that it complies with the regulatory requirements. However, on careful scrutiny, there were some lacunae in the program. For instance, as per EU GDPR, personal data must be pseudonymized or encrypted prior to transfer from one entity to another. In this case, though encryption was mentioned in the policy documents but there were no specific measures given for ensuring proper encryption of data before any transfer. Similarly, 'reasonable security practices' clause was included in customer contracts but there was no mention of any tools like firewalls or other means of protecting sensitive information which could have further strengthened the privacy protection efforts made by the company.

Thus, it is clear that XYZ did make some efforts to comply with the EU GDPR but in order to ensure full compliance, more specific measures should have been taken and all contractual obligations must be such that they clearly define the security and privacy controls that need to be put in place between customer/client and service provider. This would further give customers greater assurance of privacy protection from XYZ's services. Going forward, XYZ can consider investing in more advanced technologies like biometrics authentication etc for maximum security of data. Furthermore, the company should also ensure periodic reviews of its policy documents and contracts so as to ensure better protection of sensitive personal information.

Overall, though XYZ took some reasonable steps to protect SPI of its customers, it should have done more by introducing advanced security measures and including stringent contractual obligations for service providers.

This would have enabled the company to achieve full compliance with EU GDPR and ensure greater security of customer's personal data.

NEW QUESTION # 21

RCI and PCM

The Digital Personal Data protection Act 2023 has been passed recently. The Act shall be supported by subordinate Rules for various sections that will gradually bring more clarity into various aspects of the law.

First set of Rules are yet to be formulated and notified. A public sector bank has identified that it collects and processes personal data in physical documents and electronic form. The bank intends to assess its existing compliance level and proactively undertake an exercise to ensure compliance. Since this is the first time the bank is attempting to comply with a comprehensive privacy law, it has hired a legal expert in Privacy law to assist with initial assessment and compliance activities. As part of the initial visibility exercise the consultant identified that the bank collects and generates a significant amount of personal data in physical and digital form. The data may be upto 200 million customers' data. It is identified that customer onboarding is also done through various business correspondents in the field who collect and process personal data in physical and digital form on behalf of the bank for the purpose of opening bank accounts and this data is shared with the bank through various channels. There are upto 10 business correspondent companies that have been appointed by the bank across the country for such onboarding. These companies further appoint individual contractors on the field to face the customers. The legal consultant also identified that there are a huge number of employees and contractors engaged by the bank whose personal data is being collected and processed by the bank for HR purposes including biometric based attendance. While the intent of initial assessment was the new Act, the legal consultant has also identified that the Bank collects Aadhaar numbers (voluntary submission) from customers and employees and may be subject to Aadhaar Act compliance. It also came as a surprise that the bank wasn't aware of the data breach reporting mandate by one of the regulatory bodies under the Information Technology Act 2000 and that it was a criminal offense. The Bank generally outsources all non-core activities such as call centers which are handled by an Indian BPO company and document warehousing which is handled by another company. The Bank has also moved many of its applications to a known cloud provider as part of its digital strategy and there may be data transfer aspects associated with the same. On review of various contracts with third parties it was identified that the bank has signed standard terms of the cloud provider and has signed contracts with third parties which were in standard format of the third parties. Data protection obligations are not clear or available in these contracts. Bank leadership has been of the opinion that even the third parties should comply with the laws and robust contracts on legal compliance may not be needed. The legal consultant is not just expected to help identify gaps, assist in fixing the gaps but also to help implement controls and processes to continuously comply with evolving Rules under the new Act and also manage data protection with various third parties that may be appointed in the future.

(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 and 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 did the Bank not identify till date that they were subject to various other laws related to personal data?

What processes and controls can the legal consultant help the bank with which would help them avoid such gaps with respect to future regulations and rules issued under the new Act? Please answer with respect to the RCI practice area. (upto 250 words)

Answer:

Explanation:

See the answer in explanation below.

Explanation:

The bank has been in a hectic expansion mode and has never been subject to the regulations concerning to the data privacy. This is a huge bank with over 200 million customers, the business operations spread across many geographies and multiple operating business correspondents engaged on behalf of the bank. Thus the bank has till date not identified various other laws related with the data privacy.

The consultant has helped bank implement the following processes -

1. Document the overall business organizations, various geographical presence, various business processes, business partners.
2. Identify all related data privacy laws and regulations that pertains to the various business processes, in each geography and map the regulatory requirements with each personal information being collected/processed.
3. Define the control requirements for each and every piece of the personal information based on the the geography/jurisdiction in which it is being processed.
4. Standardize the contractual clauses with the various business associates with respect to the processing of the personal information. Assign the accountability of the adherence by way of contract amendment. These clauses needs to be included in the new contract as and when they are created.
5. Implement a organization framework comprising the legal, compliance, regulatory and business teams to establish the method by which the new regulations will be tracked and the new controls be incorporated in the overall process.
6. Implement the method to assess companies' compliance against these controls and implement the remediation methods if any non-compliance is identified.

NEW QUESTION # 22

Which of the following is not in line with the modern definition of Consent?

- A. Consent should be bundled in nature
- B. Consenting individual should have the ability to withdraw consent
- C. Consent is taken by clear and affirmative action
- D. Purpose of processing should be informed to the individual before consenting

Answer: A

Explanation:

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt,
www.stes.tyc.edu.tw, Disposable vapes

2025 Latest PDF4Test DCPLA PDF Dumps and DCPLA Exam Engine Free Share: <https://drive.google.com/open?id=1-sjNYKF8kAu8a6pLcGecVTiosDaqK3t>