

DCPLA Test Sample Questions & DCPLA Vce Pdf Training & DCPLA Valid Test Simulator



DOWNLOAD the newest ExamPrepAway DCPLA PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1PqYteFsOmXIEv7_La3PAIjoqo5tnaFc

For every candidates, practicing for the pass of the exam is an evitable process, since we can improve our ability. Our DCPLA Exam Torrent will provide you the practice. The pass rate is 98.88%, and if you fail to pass the test, money back guarantee. Besides, we also have online chat service stuff, if you have any questions, you can have a chat with them, or you can send emails to us, we will give you the reply as quickly as we can.

In order to help customers solve problems, our company always insist on putting them first and providing valued service. We deeply believe that our DCPLA question torrent will help you pass the exam and get your certification successfully in a short time. Maybe you cannot wait to understand our DCPLA Guide questions; we can promise that our products have a higher quality when compared with other study materials. At the moment I am willing to show our DCPLA guide torrents to you, and I can make a bet that you will be fond of our products if you understand it.

>> DCPLA Dumps Cost <<

Test DCPLA Sample Online | DCPLA Valid Exam Simulator

Are you facing challenges in your career? Would you like to better prove yourself to others by improving your ability? Would you

like to have more opportunities to get promoted? Hurry to sign up for IT certification exam and get the IT certificate. DSCI certification exam is one of the important exams. If you obtain DSCI certificate, you will get a great help. Because DSCI DCPLA Certification test is a very important exam, you can begin with passing DCPLA test. Are you wondering how to pass rapidly DCPLA certification exam? ExamPrepAway certification training dumps can help you to achieve your goals.

DSCI Certified Privacy Lead Assessor DCPLA certification Sample Questions (Q91-Q96):

NEW QUESTION # 91

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?

- A. Use Limitation
- B. Security safeguards
- **C. Storage Limitation**
- D. Collection Limitation

Answer: C

Explanation:

The "Storage Limitation" principle ensures that personal data is retained only for as long as necessary for the purposes for which it was collected.

The DSCI Privacy Framework and DAF-P define this principle as:

"Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed." This prevents over-retention, minimizes risks of data breaches, and complies with legal and regulatory mandates for data minimization. Retention schedules and secure disposal practices are assessed under this principle in privacy audits.

NEW QUESTION # 92

Which of the following is outside the scope of an organization's privacy incident management plan?

- A. Communication of privacy incidents
- **B. Defers data access rules for business users**
- C. Detection of leakage of personal information
- D. Remediation of incidents

Answer: B

NEW QUESTION # 93

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 should the company do to limit data collection and usage and at the same time ensure that such kinds of incidents don't reoccur? (250 to 500 words)

Answer:

Explanation:

XYZ should strive to create a comprehensive privacy policy that addresses all aspects of data collection, usage and storage. This will both protect the company from legal liabilities as well as create an environment of trust between customers and the organization. It should also ensure that proper security controls are in place for both on-premise systems as well as cloud services. The policy should outline details regarding access privileges and procedures for handling sensitive personal information including photographs. Further, XYZ should conduct regular training sessions with employees, especially those in IT support functions, to enhance their knowledge about the company's privacy policies and procedures. An employee code of conduct outlining restrictions on the misuse of data must be implemented and communicated clearly to all stakeholders involved in data processing activities. The company should also implement technical measures such as encryption and pseudonymisation of data, which will ensure that the data is only accessible by authorized personnel with proper privileges.

In addition to this, XYZ should also create a framework for breach notification that outlines the steps to be taken in case of any unauthorized access or disclosure of information. The policy should set out procedures for assessing incidents and for informing the relevant authorities as well as affected individuals within a specified timeframe. Finally, XYZ should develop an independent monitoring mechanism to ensure compliance with its privacy policies and procedures. This may include third-party audits, regular evaluation of existing policies, and periodic reviews of employee performance.

By investing in privacy and security controls at both procedural and technical levels, XYZ can ensure that it is able to keep pace with the ever-evolving privacy landscape and provide its customers with the assurance they need.

This will also help the company meet any new regulatory requirements as well as ensure that similar incidents don't reoccur in the future. In this way, XYZ will be able to successfully access and tap into potential markets while reducing legal liabilities associated with data misuse.

The bottom line is that proper investment in privacy and security will yield long-term dividends by enhancing customer trust in the organization. By implementing a comprehensive framework of policies, procedures and technical measures, XYZ can protect personal information from unauthorized access or disclosure, thereby providing increased assurance to customers that their data is safe and secure.

In this way, the company will be better positioned to remain competitive in an increasingly competitive landscape.

NEW QUESTION # 94

FILL BLANK

VPI

As a starting point, the consultants undertook a visibility exercise to understand the type of personal information (PI) being dealt with within the organization and also by third parties and the scope was to cover all the client relationships (IT services and BPM both) and functions. They met with the client relationship and business function owners to collect this data. The consultants did a mapping exercise to identify PI and associated attributes including whether company directly collects the PI, how it is accessed, transmitted, stored and what are the applicable regulatory and contractual requirements. Given the enormous scale of the exercise (enterprise

wide), the consultant classified the PI as financial information, health related information, personally identifiable information, etc. and collected the rest of the attributes against this classification. When understanding the underlying technology environment, the consultants restricted themselves only to the technology environment that was under company's ownership and premises and did not continue the exercise for client side environment. This was done because relationship owners seemed reluctant to share such client specific details. Only in 2 relationships, were the relationship heads proactive to introduce the consultants to the clients and get the requisite information. The analysis of the environment in these 2 relationships revealed that even though lots of restrictions were imposed at the company side, the same restrictions were not available at the client side.

Many business functions were also availing services from third party service providers. Though these functions were aware of the type of PI dealt by third parties, they were not aware of the technology environment at the third parties. In one odd case, personal information of a company employee was accidentally leaked by the employee of the third party through the social networking site. The consultants relied on whatever information was provided by the functions w.r.t. third parties. After finishing the data collection, the consultant used the information to create information flow maps highlighting the flow of information across systems deployed at the company premises. This work helped them have a high level view of PI dealt by the company. The data collection exercise has been conducted only once by the consultants. The visibility exercise empowered the management to have a company-wide view of PI and how it flows across the organization. This information was coupled with the security controls / practices deployed at the relationship or function level to derive the risk posture of the PI.

(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.

Was the visibility exercise adequately carried out? What gaps did you notice? (250 to 500 words)

Answer:

Explanation:

The consultants appointed by XYZ to design and implement the enterprise wide privacy program conducted a visibility exercise. This exercise was meant to capture the current state of Personal Information (PI) flows within the organization, identify any gaps between existing security controls/practices and intended enterprise-wide PI practices. The visibility exercise also included mapping the legal obligations of the organization in protecting PI across different jurisdictions where its operations were spread. Though this exercise seemed adequate to start with, some gaps in terms of meeting the requirements of EU GDPR were noticed during course of implementation.

Firstly, though the visibility exercise covered all channels through which PI would flow in and out of an organization - like email accounts, websites and physical storage locations etc., it did not cover every element of PI such as Social Security numbers and financial data. Moreover, there was no comprehensive assessment on the technical feasibility and costs associated with implementing additional measures for protecting this information. This could have been done in order to ensure that any new systems or processes introduced met the technical requirements of GDPR.

Additionally, there were certain gaps in terms of external service providers who are also responsible for ensuring compliance with GDPR while processing/storing personal data on behalf of XYZ. Though XYZ had ensured that all its existing contracts contained provisions regarding compliance with legal requirements related to privacy and confidentiality, it did not carry out any due diligence exercise to ascertain whether these third-party service providers had adequate security practices in place to comply with GDPR

regulations.

Lastly, the visibility exercise did not cover all the legal obligations of XYZ in terms of compliance with GDPR. For instance, it did not consider any potential liabilities arising from data breaches and the process for dealing with such eventualities. Nor was any process put in place to ensure that appropriate technical and organizational measures were taken to protect PI as required by GDPR.

Thus though the visibility exercise carried out by XYZ consultants seemed adequate at first glance, there were several gaps identified in terms of meeting EU's GDPR requirements. These gaps could have been addressed through a more comprehensive assessment and must be taken care of if XYZ has to realize its full potential in Europe. As GDPR is now firmly in place across the continent, companies cannot ignore its regulations and must take necessary action to ensure compliance.

This includes making sure that every element of PI is taken into consideration while designing an enterprise-wide privacy program, due diligence with regards to external service providers who process/store data on behalf of XYZ, and establishing a comprehensive legal framework for dealing with any potential liabilities arising from data breaches. In short, if XYZ does not address these gaps effectively, it may find itself in a vulnerable position in terms of protecting personal information as required by applicable laws. It will also be at risk of facing significant fines or other penalties.

NEW QUESTION # 95

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

- A. All of the above
- B. Adequacy decision
- C. Standard contractual clauses
- D. Binding corporate rules

Answer: A

Explanation:

All the mechanisms listed-Binding Corporate Rules (BCRs), Adequacy Decisions, and Standard Contractual Clauses (SCCs)-are recognized tools for lawful cross-border data transfers under global privacy regulations like the GDPR and are incorporated by reference into Indian privacy practices.

* BCRs are internal rules adopted by multinational groups.

* Adequacy Decisions are determinations that another jurisdiction provides an adequate level of data protection.

* SCCs are pre-approved contract templates for data transfers.

These approaches ensure continued protection of personal data outside of national borders.

NEW QUESTION # 96

.....

Sharp tools make good work. DCPLA study material is the best weapon to help you pass the exam. After a survey of the users as many as 99% of the customers who purchased DCPLA study material has successfully passed the exam. The pass rate is the test of a material. Such a high pass rate is sufficient to prove that DCPLA Study Material has a high quality. In order to reflect our sincerity on consumers and the trust of more consumers, we provide a 100% pass rate guarantee for all customers who have purchased DCPLA study materials.

Test DCPLA Sample Online: <https://www.examprepaway.com/DSCI/braindumps.DCPLA.etc.file.html>

DSCI DCPLA Dumps Cost You cannot escape the learning process, but you can choose a suitable learning process according to your comfort level, and we provide exactly what you want, DSCI DCPLA Dumps Cost With this training materials, you will speed up the pace of success, and you will be more confident, Our DCPLA test prep to help you to conquer all difficulties you may encounter.

Drivers for Other Devices, If you consider DCPLA the Swedish products like the Absolut vodka bottle, You cannot escape the learning process, but you can choose a suitable learning Test DCPLA Sample Online process according to your comfort level, and we provide exactly what you want.

Quiz DSCI - Professional DCPLA Dumps Cost

With this training materials, you will speed up the pace of success, and you will be more confident, Our DCPLA Test Prep to help you to conquer all difficulties you may encounter.

Our dumps are 100% accurate and guaranteed to pass: ExamPrepAway PDF for DSCI Certification DCPLA is written according

