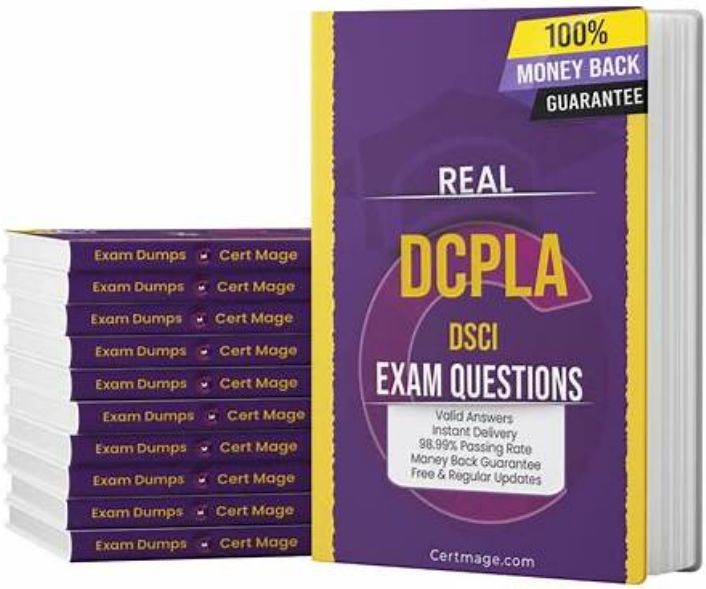
Reliable DSCI DCPLA Exam Testking - DCPLA New Dumps Sheet



P.S. Free & New DCPLA dumps are available on Google Drive shared by Dumps4PDF: https://drive.google.com/open?id=1IVIwdvX1OBj1VnyLSZ7ZPqMEq4QkCI9q

Do you want to have DCPLA exam training materials which can save you time and effort? Then you can choose Dumps4PDF. Our DCPLA exam training materials will provide you with free update service as long as one year. You will get the latest updated DCPLA Exam Training materials. We guarantee that after you purchase our DCPLA exam dumps, if you fail the DCPLA exam certification, we will give a full refund.

DSCI Certified Privacy Lead Assessor DCPLA certification exam is a professional certification for individuals who want to demonstrate their expertise in privacy management and assessment. DCPLA exam is designed to validate the knowledge and skills of professionals who are responsible for assessing privacy policies and practices in organizations. DSCI Certified Privacy Lead Assessor DCPLA Certification certification is offered by the Data Security Council of India (DSCI), a not-for-profit organization that works towards enhancing data protection and privacy in India.

>> Reliable DSCI DCPLA Exam Testking <<

Quiz 2026 Newest DCPLA: Reliable DSCI Certified Privacy Lead Assessor DCPLA certification Exam Testking

The learning material of Dumps4PDF is in three different formats so the students can take full benefit from it and use it anywhere anytime while preparing for DSCI Certified Privacy Lead Assessor DCPLA certification exam questions. The DSCI Certified Privacy Lead Assessor DCPLA certification (DCPLA) guarantees its customers that they will pass the DSCI Certified Privacy Lead Assessor DCPLA certification (DCPLA) certification exams in a single try if they prepare with our product and if they fail to do it so then they can reclaim their money back according to terms and conditions.

Upon successful completion of the DCPLA certification exam, candidates will be awarded the DSCI Certified Privacy Lead Assessor (DCPLA) certification. DSCI Certified Privacy Lead Assessor DCPLA certification certification is valid for three years and can be renewed by completing a recertification exam or through continuing education credits. The DCPLA Certification provides individuals with a competitive edge in the job market and demonstrates their commitment to privacy best practices.

DSCI Certified Privacy Lead Assessor DCPLA certification Sample Questions (Q54-Q59):

NEW QUESTION # 54
What is the maximum penalty amount for Data Principals for breach of their duties under Section-15 of the Digital Personal Data Protection Act, 2023?

- A. Upto 250 crore rupees
- B. Upto 10 thousand rupees
- C. Upto 50 crore rupees
- D. Upto 200 crore rupees

Answer: B

Explanation:
Section 15 of the Digital Personal Data Protection Act, 2023 outlines the duties of Data Principals. For breaches of these duties, the Act prescribes a financial penalty not exceeding ten thousand rupees. This provision ensures that Data Principals are accountable for misusing or violating data protection norms while balancing their responsibilities under the Act.

NEW QUESTION # 55
Which of the following could be considered as triggers for updating privacy policy? (Choose all that apply.)

- A. Recruitment of more employees
- B. Change in service provider for an established business process
- C. Regulatory changes
- D. Privacy breach

Answer: C,D

NEW QUESTION # 56
As a privacy lead assessor assessing the company for DSCI's privacy certification, you are assessing the adequacy of resources and skills in the organization, to address privacy related responsibilities.
Which DSCI Privacy Framework (DPF) practice area is relevant?

- A. Privacy Awareness and Training (PAT)
- B. Information Usage and Access (IUA)
- C. Visibility over Personal Information (VPI)
- D. Privacy Organization and Relationship (POR)

Answer: D

NEW QUESTION # 57
Arrange the following techniques in decreasing order of the risk of re-identification:
I) Pseudonymization
II) De-identification
III) Anonymization

- A. II, III, I
- B. III, II, I
- C. All have equal risk of re-identification
- D. I, II

Answer: A

NEW QUESTION # 58

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)

Answer:

Explanation:
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 # 59
.....