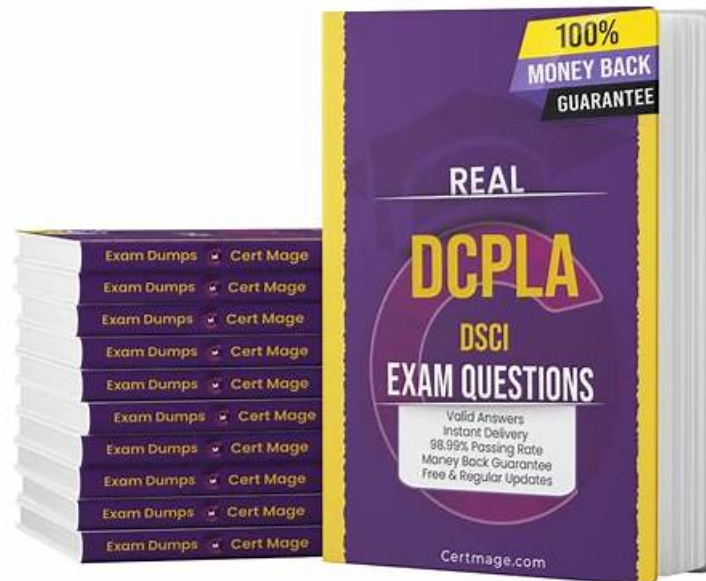


DCPLA Exam Consultant - Mock DCPLA Exam



P.S. Free 2026 DSCI DCPLA dumps are available on Google Drive shared by ExamBoosts: https://drive.google.com/open?id=1ZMLbBF2ZCZY_1lP9vpuSxWnsp2ctYjq1

With these adjustable DSCI Certified Privacy Lead Assessor DCPLA certification (DCPLA) mock exams, you can focus on weaker concepts that need improvement. This approach identifies your mistakes so you can remove them to master the DSCI Certified Privacy Lead Assessor DCPLA certification (DCPLA) exam questions of ExamBoosts give you a comprehensive understanding of DCPLA Real Exam format. Self-evaluation by taking practice exams makes your DSCI DCPLA exam preparation flawless and strengthens enough to crack the test in one go.

The DCPLA certification exam is designed for professionals who are involved in privacy assessments and management, including privacy officers, compliance officers, legal professionals, and IT professionals. DSCI Certified Privacy Lead Assessor DCPLA certification certification program covers various aspects of privacy assessment and management, including privacy laws and regulations, privacy risk assessment, privacy impact assessment, privacy program development and implementation, and privacy audit and monitoring. DSCI Certified Privacy Lead Assessor DCPLA Certification certification exam is a two-day program, which includes both theoretical and practical components.

>> DCPLA Exam Consultant <<

Mock DCPLA Exam - DCPLA Training Tools

You can also trust ExamBoosts DCPLA exam practice questions and start preparation with complete peace of mind and satisfaction. The DCPLA Exam Questions are designed and verified by experienced and renowned DSCI exam trainers. They work collectively and strive hard to ensure the top quality of DCPLA Exam Practice questions all the time.

DSCI Certified Privacy Lead Assessor DCPLA certification Sample Questions (Q66-Q71):

NEW QUESTION # 66

Certification once granted, will be valid for period of _____ years subject to surveillance assessments.

- A. 0

- B. 1
- C. 2
- D. 3

Answer: D

NEW QUESTION # 67

Categorise the following statement:

"For an identified data leakage scenario, security team is struggling to configure rules."

- A. Enforcement
- B. Demonstration
- C. Visibility
- D. Capability

Answer: D

Explanation:

The statement reflects an organization's difficulty in operationalizing privacy safeguards in response to a known threat scenario. According to the DSCI Assessment Framework for Privacy (DAF-P), "Capability" refers to an organization's ability to implement and maintain technical, procedural, and administrative controls effectively.

A struggling security team in configuring rules for a known leakage scenario indicates a gap in technical expertise or resources, which directly correlates with a lack of "Capability." This category assesses how prepared an organization is in deploying privacy controls, managing incidents, and aligning security technologies with privacy requirements.

Thus, the challenge in configuring protective rules is best categorized under "Capability" as it denotes a functional inadequacy in handling privacy-related incidents.

NEW QUESTION # 68

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 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.

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:

See the answer in explanation below.

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 # 69

Privacy enhancing tools aim to allow users to take one or more of the following actions related to their personal data that is sent to, and used by online service providers, merchants or other users:

- I) Increase control over their personal data
- II) Choose whether to use services anonymously or not
- III) Obtain informed consent about sharing their personal data
- IV) Opt-out of behavioral advertising or any other use of data

- A. I, II, III and IV
- B. Only I and II
- C. Only II
- D. Only I

Answer: A

