便利なDCPLA学習教材と信頼的なDCPLA試験時間

さらに、Japancert DCPLAダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1MzoBwOfKzKU1zytIjAPlGL5eAV2SnSxq

かねてIT認定試験資料を開発する会社として、高品質のDSCI DCPLA試験資料を提供したり、ビフォワ.アフタサービスに関心を寄せたりしています。我々社の職員は全日であなたのお問い合わせを待っております。何の疑問があると、弊社の職員に連絡して問い合わせます。一年間で更新するなる、第一時間であなたのメールボックスに送ります。

DSCI DCPLA（DSCI認定プライバシーリードアセッサー）認定は、プライバシーとデータ保護に特化した専門家向けのグローバルに認められた認定プログラムです。この認定は、プロフェッショナルがプライバシーリスクを評価･管理するために必要な知識とスキルを備えるよう設計されています。このプログラムでは、法律や規制、データガバナンス、リスク管理、インシデント管理など、プライバシーとデータ保護のさまざまな側面をカバーしています。

>> DCPLA学習教材 <<

DCPLA試験時間 & DCPLA問題集

DCPLA試験資格証明書を取得することは難しいです。でも、DSCI　DCPLA復習教材を選ばれば、試験に合格することは簡単です。DCPLA復習教材の内容は全面的で、価格は合理的です。そして、DSCIはお客様にディスカウントコードを提供でき、DCPLA復習教材をより安く購入できます。

DSCI Certified Privacy Lead Assessor（DCPLA）は、世界的に認められた認定であり、プロフェッショナルが組織内のプライバシーリスクを評価および管理することを可能にします。DCPLA試験は、候補者にプライバシーリスクを特定し、プライバシーコントロールを設計および実装し、関連する国際的なプライバシー法律および規制に準拠するために必要な知識とスキルを提供します。この認定は、NASSCOMによって設立された非営利団体であるData Security Council of India（DSCI）によって提供され、グローバル市場におけるプライバシープロフェッショナルの需要の増加に対応するように設計されています。

DSCI Certified Privacy Lead Assessor DCPLA certification 認定 DCPLA 試験問題 (Q98-Q103):

質問 # 98
The concept of data adequacy is based on the principle of _____.

- A. Essential assessment
- B. Dissimilarity of legislations

- C. Adequate compliance
- D. Essential equivalence

正解：D

解説：
Data adequacy is a concept primarily referenced under international data transfer mechanisms, especially in GDPR and mirrored in Indian and global privacy frameworks. The idea is that a country can receive personal data from another country if it ensures an "adequate level of protection".
This level is determined not by exact replication of laws but by their "Essential Equivalence" to the originating country's standards. The principle of "Essential Equivalence" means that although the laws do not have to be identical, they must offer comparable protection in practice. This is the benchmark used by authorities like the EU Commission and reflected in frameworks including DPF©.

質問 # 99
_____ calls for inclusion of data protection from the onset of the designing of systems.

- A. Agile Model
- B. Logical Design
- C. Safeguarding Approach
- D. Privacy by Design

正解：D

質問 # 100
What is a Data Subject? (Choose all that apply.)

- A. A company providing PI of its employees for processing
- B. An individual who provides his/her data/information for availing any service
- C. An individual whose data/information is processed
- D. An individual who collects data from illegitimate sources
- E. An individual who processes the data/information of individuals for providing necessary services

正解：B、C

質問 # 101
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 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 be the learning for the company going forward? What should the consultants suggest? (250 to
500 words)
D. None of the above

正解：

解説：
See the answer in explanation below.
Explanation:
The consultants should suggest a comprehensive and integrated privacy program for the company which addresses the current regulatory requirements while being proactive in anticipating any changes to these regulations. The program should be effective, flexible, cost-efficient and easy to understand and implement.
To begin with, the program should involve an assessment of all existing processes and procedures that are related to personal data processing in order to identify potential areas of risk. The potential risks along with recommended mitigating controls should then be documented in a Privacy Impact Assessment (PIA) report.
This will enable the organization to assess its compliance level against applicable regulations.
It is also important for XYZ to have strong Data Governance policies and procedures along with appropriate organizational structures and accountability mechanisms in place. This will include a Data Privacy Officer (DPO) who is responsible for overseeing the compliance program and being the point of contact for data protection supervisory authorities. The DPO should be part of the management team and report to the CIO's office as well as senior-level executives.
A consultant should also recommend data minimization, pseudonymization, encryption, and other security measures to protect personal information. In addition, they can recommend regular privacy awareness training sessions for employees, so that they are up-to-date on changes in regulations and understand how their role impacts data privacy and security. Lastly, all systems and processes should be monitored and audited to ensure compliance with relevant regulations.
As a result, consultants should provide clients in the EU and US with an integrated and comprehensive privacy program that provides the necessary assurances and protects sensitive data from unauthorized access or misuse. By leveraging outsourcing opportunities in the healthcare sector in the US, XYZ could potentially gain competitive advantage.

質問 # 102
With respect to privacy monitoring and incident management process, which of the following should be a part of a standard incident handling process?
I) Incident identification and notification
II) Investigation and remediation
III) Root cause analysis
IV) User awareness training on how to report incidents

- A. I, II and III
- B. All of the Above
- C. III and IV

- D. I and II

正解：B

解説：
DSCI Privacy Framework recommends a holistic approach to incident management which includes:
* Identification and timely notification of incidents (I)
* Thorough investigation and effective remediation measures (II)
* Conducting root cause analysis to prevent recurrence (III)
* Educating users on how to recognize and report incidents (IV)
Each of these components plays a critical role in reducing risk exposure and ensuring continual improvement of the privacy program.

質問 # 103
.....