DSCI DCPLA Practice Questions

Shared by Ward on 28-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following are key contributors that would enhance the complexity in implementing security measures for protection of personal information? (Choose all that apply.)

Options:

A- Data collection through multiple modes and channels
B- Evolution of nimble and flexible business processes affecting access management
C- Regulatory requirements to issue privacy notice and data breach notification in specified format
D- None of the above

Answer:

A, B

Explanation:

The complexity of implementing data security for personal information is often influenced by operational and architectural factors such as:

A: Collecting data through various channels like web forms, mobile apps, customer support, etc., which introduces complexity in tracking and securing each channel.

B: Flexible and dynamic business processes that evolve rapidly can complicate access management due to frequent changes in user roles, workflows, and data access needs.

While regulatory requirements (C) do impact privacy governance, they do not directly contribute to the complexity of implementing technical security measures.

Question 2

Question Type: MultipleChoice

Section 43A of the Information Technology (Amendment) Act, 2008 holds_____ accountable for having reasonable security practices and procedures in place to protection sensitive personal data.

Options:

A- Government
B- Body corporates
C- Government and body corporates alike
D- Personal Information Security

Answer:

B

Explanation:

Section 43A of the IT (Amendment) Act, 2008 states:

''When a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices, and thereby causes wrongful loss or wrongful gain, such body corporate shall be liable to pay damages.''

This clearly places the onus of compliance and data security on body corporates.

Question 3

Question Type: MultipleChoice

SIMULATION

[Scenario Based Questions]

PPP

Based on the visibility exercise, the consultants created a single privacy policy applicable to all the client relationships and business functions. The policy detailed out what PI company deals with, how it is used, what security measures are deployed for protection, to whom it is shared, etc. Given the need to address all the client relationships and business functions, through a single policy, the privacy policy became very lengthy and complex. The privacy policy was published on company's intranet and also circulated to heads of all the relationships and functions. W.r.t some client relationships, there was also confusion whether the privacy policy should be notified to the end customers of the clients as the company was directly collecting PI as part of the delivery of BPM services. The heads found it difficult to understand the policy (as they could notdirectly relate to it) and what actions they need to perform. To assuage their concerns, a training workshop was conducted for 1 day. All the relationship and function heads attended the training. However, the training could not be completed in the given time, as there were numerous questions from the audiences and it took lot of time to clarify.

(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 Afric

a. 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 are key issues in the policy design process? (upto 250 words)

Options:

A- See the answer in explanation below

Answer:

A

Explanation:

The PI policy (or for that matter any policy) needs to be purpose driven, clear, consize, easily accessible to be effective. Ideally the PI policy controls needs to be implemented as a part of the overall operations process so that the implementation of this policy is automatic. In this case, the issues wiuth the policy design process was -

1. the policy was a generic and common policy for all the business functions/unit. Such policies become lengty, complex and deters the policy subjects from adopting it.

2. All the client relationships and business functions are unique. They differ in their purpose, objectives, process and hence also in the type of the information then collect and process. The policy should be easy and customized for each department.

3. The policy is published on the intraned portal. There is no guarantee that the policy is read and consumed by all desired stakeholder. As opposed to this, this policy matter should be made relevant and customized for the stakeholders and be PUSHED to them agains them PULLING it at their discretion.

4. The roles and responsibilities, accountability and penalty for each stakeholders should be defined clearly so there is no confusion in the adherence to the policy.

5. The training workshop was generic and was short. It was not completed in time. the training program should be customized and contextual to the department people that are being trained. the program should be conducted in a very professional environment and method.

6. Since the policy, purpose, roles and responsibilities were not clear, the training program did not go well.

Question 4

Question Type: MultipleChoice

What are the criteria for deciding the role of Data Fiduciary? Tick all that apply.

Options:

A- Data Fiduciary is the one who decides the means of personal data processing
B- Data Fiduciary is the one who acts on behalf of data processor
C- Data Fiduciary is the one who stores the personal data
D- Data Fiduciary is the one who decides the purposes of personal data processing

Answer:

A, D

Explanation:

Under the Digital Personal Data Protection Act, 2023, a Data Fiduciary is defined as any person who alone or in conjunction with other persons determines the purpose and means of processing personal data. Therefore, A and D are correct.

Option B is incorrect because acting on behalf of a processor implies a sub-processor or related role, not a fiduciary.

Option C is incorrect because mere storage does not make an entity a Data Fiduciary.

P2P exams

Question 5

Question Type: MultipleChoice

Following aspects can serve as inputs to a privacy organization for ensuring privacy protection:

I) Privacy related incidents detected/reported

II) Contractual obligations

III) Organization's exposure to personal information

IV) Regulatory requirements

Options:

A- I, II and III
B- II and IV
C- I, II, III and IV
D- None of the above, as privacy and compliance protection mechanisms are evolved based only on organization's privacy policies and procedures

Answer:

C

Explanation:

The DSCI Privacy Framework recommends that a privacy program must be tailored based on

several practical and operational inputs. These include:

Reported privacy incidents (to identify risk patterns and weaknesses)

Contractual obligations (which dictate processing standards for third parties)

Exposure to personal information (understanding where and how personal data is processed)

Regulatory compliance (to ensure adherence to national and international laws)

All four listed aspects contribute to the risk-based and dynamic implementation of privacy strategies within an organization.

Question 6

Question Type: MultipleChoice

Which option best measures can an organization implement to establish regulatory compliance intelligence? (Choose all that apply.)

Options:

A- Establish a process that keeps a track of applicable legal and regulatory changes
B- Identify the liabilities imposed by the regulations with respect to specific data elements
C- Ensure that a mechanism exists for quick and effective provisioning, de-provisioning and authorization of access to information or systems which are exposed to data
D- Ensure that knowledge with respect to legal and regulatory compliances is managed effectively

Answer:

A, B, D

Explanation:

According to the DSCI Privacy Framework, the practice area of ''Regulatory Compliance Intelligence (RCI)'' is dedicated to helping organizations:

Continuously track evolving laws and regulations (A)

Map these requirements and associated liabilities to data elements and processing activities (B)

Develop internal knowledge management systems for compliance obligations (D)

Option C, however, relates more to access control and information security, which is typically addressed under technical and security safeguard controls, not under the RCI practice area.

Question 7

Question Type: MultipleChoice

'Map the legal and compliance requirements to each data element that an organization is dealing with in all of its business processes, enterprise and operational functions, and client relationships.' This an imperative of which DPF practice area?

Options:

A- Visibility over Personal Information (VPI)
B- Privacy Organization and Relationship (POR)
C- Regulatory Compliance Intelligence (RCI)
D- Privacy Policy and Processes (PPP)

Answer:

C

Explanation:

The DPF's ''Regulatory Compliance Intelligence (RCI)'' practice area is focused on identifying and mapping applicable legal and compliance requirements to the specific data elements across business processes. This enables organizations to operationalize compliance obligations by linking them directly with the data they manage.

RCI helps ensure that every data flow or processing activity has a mapped legal basis and complies with jurisdictional requirements.

Question 8

Question Type: MultipleChoice

SIMULATION

[Scenario Based Questions]

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 Afric

a. 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)

Options:

A- See the answer in explanation below

Answer:

A

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.

Question 9

Question Type: MultipleChoice

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

Options:

A- Adequate compliance
B- Dissimilarity of legislations
C- Essential equivalence
D- Essential assessment

Answer:

C

Explanation:

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.

Question 10

Question Type: MultipleChoice

Categorise the following statement:

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

Options:

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

Answer:

B

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.

To Get Premium Files for DCPLA Visit

https://www.p2pexams.com/products/dcpla

For More Free Questions Visit

https://www.p2pexams.com/dsci/pdf/dcpla

