# KillTest

Higher Quality, Better Service!

# Q&A

http://www.killtest.com

We offer free update service for one year.

**Exam** : **DCPLA**

**Title** : DSCI Certified Privacy Lead Assessor

**Version** : DEMO

1.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. Only I
B. Only I and II
C. I, II, III and IV
D. Only II
**Answer:** C

2.CORRECT TEXT
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 lient, 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.
What should be the learning for the company going forward? What should the consultants suggest? (250 to 500 words)

**Answer:**

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 & 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 & 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 & processes should be monitored & audited to ensure compliance with relevant regulations.

As a result, consultants should provide clients in the EU and US with an integrated & 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.

3.Classify the following scenario as major or minor non-conformity.
“The organization has a very mature information security policy. Lately, the organization has realized the need to focus on protection of PI. A formal PI identification exercise was done for this purpose and a mapping of PI and security controls was done. The organization has also put in place data masking technology in certain functions where the SPI was accessed by employees of a third party. However, the organization is yet to include PI specifically in its risk assessment exercise, incident management, testing, data classification and security architecture programs.”
A. Major
B. Minor
C. Both Major & Minor
D. None of the above
**Answer:** A

4.CORRECT TEXT
FILL BLANK
PIS
The company has a well-defined and effectively implemented security policy. As in case of access control, the security controls vary in different client relationships based on the client requirements but certain basic or hygiene security practices / controls are implemented organization wide. The consultants have advised the information security function to realign the company’s security policy, risk assessment, data classification, etc to include privacy aspects. But the consultants are struggling to make information security function understand what exact changes need to be made and the security function itself is unable to figure it out.
(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.
Can you please guide the information security function to realign company’s security initiatives to include privacy protection, keeping in mind that the client security requirements would vary across relationships? (250 to 500 words)

**Answer:**

The information security function of XYZ needs to realign the company’s security initiatives to include privacy protection and make sure that it meets its client’s requirements. The Information Security team must understand the legal and regulatory requirements for data privacy for each region in which XYZ operates, as well as industry standards such as ISO 27001/2 or NIST 800-53. This will help ensure that the organization is complying with applicable laws and regulations, while also helping build trust with clients by demonstrating that they take privacy seriously.
The Information Security team should also identify the most important risks associated with data privacy in order to determine what additional measures need to be taken in order to protect sensitive data from misuse or loss. The team should then assess the appropriate risk management and privacy controls to ensure that the data is being managed in a secure manner. This could include encryption of sensitive data, access control measures such as role-based permissions, and regular reviews of user access rights to ensure proper security protocols are being followed.
In addition, XYZ should create an internal privacy policy which outlines its commitment to protecting the privacy of customers and employees. The policy should be reviewed periodically to ensure it meets changing regulatory requirements and industry standards. The policy must also be communicated to all staff members so they know what their responsibilities are with regards to protecting personal data.
Finally, XYZ should have a robust incident response plan in place for when breaches or unauthorized access occur. This should cover procedures for detecting, investigating, and responding to potential data breaches. It should also include measures to prevent future incidents and ensure that customer data is protected going forward.
By taking these measures, XYZ will be able to meet its client’s security requirements while also demonstrating its commitment to protecting the privacy of their customers. This can help build trust with existing clients as well as new ones, making it easier for them to do business with the company. In addition, a comprehensive privacy protection program can help protect XYZ from costly legal or regulatory penalties in case of a data breach. Therefore, it is crucial for XYZ to invest in robust privacy protection initiatives in order to realize the full potential of the market.

5.The concept of data adequacy is based on the principle of _____.
A. Adequate compliance
B. Dissimilarity of legislations
C. Essential equivalence
D. Essential assessment
**Answer:** C