Free Questions for DCPLA by certsdeals

Shared by Farley on 14-12-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

FILL BLANK

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 not directly 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 & 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.

Given the confusion among relationship and function heads, how would you proceed to address the problem and ensure that policy is well understood and deployed? (250 to 500 words)

Options:

A- Explanation:

In order to address the confusion among relationship and function heads, it is important to ensure that the privacy policy is effectively communicated and understood by all stakeholders. The following steps can be taken towards this end:

1. Awareness Campaigns - In order to educate the stakeholders about the importance of data privacy, various awareness campaigns should be launched through digital media, print media, and seminars. These campaigns must include topics such as why data privacy is important, the consequences of not adhering to the policy, and how to comply with it.
2. Training - In addition to awareness campaigns, proper training should be provided to all stakeholders on data privacy policies and procedures. The training should also focus on best practices such as secure coding, encryption techniques etc., so that they understand the importance of these security measures in protecting data from unauthorized access.
3. Policies and Procedures - All stakeholders should have access to a clear set of policies and procedures governing their actions related to data privacy. Such guidelines should include information about the types of sensitive information which needs to be kept confidential, what constitutes a violation of the policy, and how to take corrective measures if a violation occurs.
4. Auditing - The effectiveness of all the policies and procedures should be regularly audited in order to ensure that the data privacy policy is being followed properly. Any discrepancies or violations must be reported immediately so that appropriate action can be taken.
5. Reporting Mechanism - A reporting mechanism should also be put into place for stakeholders to report any suspected errors or breaches in data privacy policies. This will help in identifying potential risks early on and taking corrective action as soon as possible.

These initiatives will not only reduce confusion among relationship and function heads but will also help build trust with customers by ensuring proper implementation of enterprise-wide privacy program, which in turn will help the company in leveraging outsourcing opportunities. Lastly, by following all these measures, the company will be able to demonstrate its commitment towards privacy and create a secure environment for its customers.

In conclusion, in order to ensure that policy is well understood and deployed, it is important to take appropriate steps such as launching awareness campaigns, providing training to stakeholders on data privacy policies, auditing policies and procedures regularly, and setting up a reporting mechanism for errors or breaches. Doing so will reduce confusion among relationship and function heads and help build trust with customers by ensuring proper implementation of an enterprise-wide privacy program.

Answer:

A

Question 2

Question Type: MultipleChoice

FILL BLANK

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 not directly 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 & 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.

Do you agree with company's decision to have single privacy policy for all the relationships and functions? Please justify your view. (250 to 500 words)

Options:

A- Explanation:

Yes, I agree with the company's decision to have a single privacy policy for all its relationships and functions. Having a unified privacy policy allows the organization to communicate consistently across multiple channels of communication with customers, partners and vendors. It also ensures that all stakeholders are aware of their rights when dealing with personal data and makes it easier for them to understand their responsibilities when handling such information.

Moreover, having a standardized privacy policy helps to protect the company from potential legal repercussions due to inadequate protection of confidential data. The need for comprehensive protection is especially important in this age where cyber-attacks are becoming increasingly frequent and sophisticated. By putting in place a consistent framework that governs how any organization handles sensitive information can help reduce the risks associated with data breaches.

By demonstrating that the company takes strong measures to protect its customers' personal information, a single privacy policy can help boost the company's reputation and build trust with customers. Compliance with a variety of regulatory requirements is especially important for companies operating in regulated industries, such as banking and healthcare.

In addition, having a unified privacy policy allows organizations to maintain control over how their data is stored and processed. By monitoring who has access to confidential information, companies can identify any potential security vulnerabilities before they are exploited by malicious actors.

To conclude, I support XYZ's decision to have one privacy policy for all its relationships and functions. Having a unified privacy policy can help the organization protect itself from potential legal risks, boost its reputation and maintain control over how data is stored and used. All in all, it is an important step to ensure that customer data is always kept safe and secure.

Answer:

A

Question 3

Question Type: MultipleChoice

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 & 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)

Options:

A- 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.

Answer:

A

Question 4

Question Type: MultipleChoice

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 & 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- 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 & 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.

Answer:

A

Question 5

Question Type: MultipleChoice

FILL BLANK

RCI and PCM

In April 2011, the rules were issued under Section 43A of the IT Act by the Government of India and the 'body corporates' were required to comply with these rules. The Corporate legal team tried to understand and interpret the rules but struggled to understand its applicability esp. to client relationships and business functions. So, the company hired an IT Act legal expert to advise them on the Section 43A rules.

To start with, the company identified the PI dealt with by business functions as part of the earlier visibility exercise, but it wanted to reassure itself. Therefore, a specific exercise was conducted to revisit 'sensitive personal information' dealt by business functions. It was realized that the company collects lot of SPI of its employees and therefore 'reasonable security practices' need to be adhered to by the functions that deal with SPI. It was also ascertained that many of this SPI is being dealt by third parties, some of which are also located outside Indi

a. To meet the requirements of the rules, the company reviewed all the contracts and inserted a clause -- 'the service provider shall implement reasonable security practices and procedures as per the IT (Amendment) Act, 2008'. Some of the large service providers were ISO 27001 certified and they claimed that they fulfill the requirements of 'reasonable security practices'. However, some SME service providers did not understand what would 'reasonable security practices' imply and requested the company to clarify, which referred them to Rule 8 of the Section 43A. Some small scale service providers expressed their unwillingness to get ISO certified, given the costs involved.

(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.

Did the company take sufficient steps to protect SPI dealt by its service providers and ensure that it complies with the regulatory requirements? Was referring to 'reasonable security practices' sufficient in the contracts or the company should have also considered some other measures for privacy protection as well? (250 to 500 words)

Options:

A- Explanation:
The consulting arm of XYZ developed a comprehensive privacy program in line with the company's goal to leverage its existing technology infrastructure, resources and capabilities for protecting data. The program had three parts -- awareness and training, policy development and implementation. On the awareness front, extensive training was conducted for employees on various aspects of privacy including GDPR compliance. This was followed by the development and rollout of an enterprise-wide privacy policy which clearly defined the various steps to be taken to protect sensitive personal information (SPI) such as encryption, access controls etc. After this, customer contracts were reviewed for appropriate protection clauses and service providers were made to sign 'reasonable security practices' clauses in their contractual obligations as specified in EU GDPR.

At first glance, it seemed that XYZ had taken adequate steps to protect SPI dealt by its service providers and ensure that it complies with the regulatory requirements. However, on careful scrutiny, there were some lacunae in the program. For instance, as per EU GDPR, personal data must be pseudonymized or encrypted prior to transfer from one entity to another. In this case, though encryption was mentioned in the policy documents but there were no specific measures given for ensuring proper encryption of data before any transfer. Similarly, 'reasonable security practices' clause was included in customer contracts but there was no mention of any tools like firewalls or other means of protecting sensitive information which could have further strengthened the privacy protection efforts made by the company.

Thus, it is clear that XYZ did made some efforts to comply with the EU GDPR but in order to ensure full compliance, more specific measures should have been taken and all contractual obligations must be such that they clearly define the security and privacy controls that need to be put in place between customer/client and service provider. This would further give customers greater assurance of privacy protection from XYZ's services. Going forward, XYZ can consider investing in more advanced technologies like biometrics authentication etc for maximum security of data. Furthermore, the company should also ensure periodic reviews of its policy documents and contracts so as to ensure better protection of sensitive personal information.

Overall, though XYZ took some reasonable steps to protect SPI of its customers, it should have done more by introducing advanced security measures and including stringent contractual obligations for service providers. This would have enabled the company to achieve full compliance with EU GDPR and ensure greater security of customer's personal data.

Answer:

A

Question 6

Question Type: **MultipleChoice**

FILL BLANK

MIM

The company has a well-defined and tested Information security monitoring and incident management process in place. The process has been in place since last 10 years and has matured significantly over a period of time. There is a Security Operations Centre (SOC) to detect security incidents based on well-defined business rules.

The security incident management is based on ISO 27001 and defines incident types, alert levels, roles and responsibilities, escalation matrix, among others. The consultants advised company to realign the existing monitoring and incident management to cater to privacy requirements. The company consultants sought help of external privacy expert in this regard.

(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 & 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.

If you were the privacy expert advising the company, what steps would you suggest to realign the existing security monitoring and incident management to address privacy requirements especially those specific to client relationships? (250 to 500 words)

Options:

A- Explanation:

As an external privacy expert, the first step I would suggest for XYZ company is to conduct a detailed assessment of their existing security monitoring and incident management processes. This should include an analysis of how data is collected, stored, and accessed; what kind of policies are currently in place; and any other relevant security measures. It should also identify areas where additional process or technical changes may be required to meet privacy requirements.

Once the initial assessment has been completed, I would recommend that XYZ take steps to ensure that its processes align with applicable laws and regulations regarding data protection, such as EU GDPR. For example, they should update their policies around data collection and storage so that they comply with GDPR's requirements on consent and purpose limitation. Additionally, XYZ should ensure that their systems are secure and only authorized personnel can access the data.
Also I would suggest that XYZ develop a comprehensive incident response plan, indicating how they will address any data breaches or other privacy incidents. The plan should include steps for notification to affected individuals or organizations, containment of the incident, investigations into its cause and scope, and remediation efforts to prevent similar incidents in the future.
Lastly I would recommend that XYZ review their client contracts to ensure that they clearly describe the company's commitments regarding data protection and security measures. This could include GDPR-compliant language on consent forms as well as clauses committing to regularly audit and update processes as necessary. These contractual terms will help protect both XYZ and their clients in the event of a privacy breach.
In conclusion, implementing these steps will help XYZ establish an effective privacy program that meets all applicable legal requirements, protects their clients' data, and provides them with a competitive edge in the market. Additionally, it will ensure that they remain compliant and have appropriate measures in place to address any potential issues. By taking these proactive measures now, XYZ can ensure that they continue to successfully operate in both the EU and US markets while protecting the privacy of its customers.

Answer:

A