

DCPLA試験の準備方法 | 実際のDCPLA合格率試験 | 完璧なDSCI Certified Privacy Lead Assessor DCPLA certification無料問題



無料でクラウドストレージから最新のGoShiken DCPLA PDFダンプをダウンロードする：
https://drive.google.com/open?id=1TVbdd814Bi4Kn6EFwCRbXiF6txL_8OKy

GoShikenは100%の合格率を保証するだけでなく、1年間の無料なオンラインのDCPLA問題更新を提供しております。最新の資源と最新の動態が第一時間にお客様に知らせいたします。何の問題があったらお気軽に聞いてください。

あなたは自分の職場の生涯にユニークな挑戦に直面していると思ったら、DSCIのDCPLAの認定試験に合格することが必要になります。GoShikenはDSCIのDCPLAの認定試験を真実に、全面的に研究したサイトです。GoShikenのユニークなDSCIのDCPLAの認定試験の問題と解答を利用したら、試験に合格することがたやすくなります。GoShikenは認証試験の専門的なリーダーで、最全面的な認証基準のトレーニング方法を追求して、100パーセントの成功率を保証します。GoShikenのDSCIのDCPLAの試験問題と解答は当面の市場で最も徹底かつ正確かつ最新な模擬テストです。それを利用したら、初めに試験を受けても、合格する自信を持つようになります。

>> DCPLA合格率 <<

DSCI DCPLA Exam | DCPLA合格率 - 最高のDCPLA無料問題を提供する

お客様は、DCPLA試験問題を迅速に受けることができます。クライアントは、製品のバージョンを選択し、正しいメールに記入し、DCPLA有用なテストガイドの料金を支払うだけです。その後、彼らは5〜10分でメールを受け取ります。クライアントがリンクをクリックすると、すぐにDCPLA学習資料を使用できます。クライアントがメールを受信できない場合は、オンラインカスタマーサービスに連絡して、問題の解決を支援します。購入手順は簡単で、DCPLA学習ツールの配布は迅速です。

DSCI Certified Privacy Lead Assessor DCPLA certification 認定 DCPLA 試験問題 (Q91-Q96):

質問 #91

Which of the following does the 'Privacy Strategy and Processes' layer in the DPF help accomplish? (Choose all that apply.)

- A. Visibility over Personal Information
- B. Personal Information Security
- C. Information Usage and Access
- D. Regulatory Compliance Intelligence
- E. Privacy Policy and Processes

正解: A、D、E

解説:

The 'Privacy Strategy and Processes' layer within the DSCI Privacy Framework (DPF©) is designed to support the development of:

- * A structured privacy governance model
- * Visibility over personal information and processing flows (A)
- * Organizational privacy policies and operational processes (B)
- * Mechanisms for understanding and addressing regulatory obligations (C) While Information Usage and Access (D) and Personal Information Security (E) are important aspects of privacy management, they fall under different layers such as 'Data Life Cycle Management' and 'Security Controls' respectively, rather than the Strategy and Processes layer.

質問 # 92

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

- A. Government
- B. Body corporates
- C. None of the above
- D. Government and body corporates alike

正解: D

質問 # 93

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 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.

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)

正解:

解説:

See the answer in explanation below.

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.

質問 # 94

Which of the following is the most effective way of ensuring the conformity to legal regulations from the business functions, processes and relationships?

- A. Deploying desktop screens articulating information on regulations and responsibility of the organisation
- B. Providing a special section on regulatory and compliance requirements on internal portal, providing access to respective owner of functions, processes and relationships
- C. Conducting classroom training and awareness sessions on regulatory and compliance requirements
- D. Customised delivery of information on regulatory and compliance information to the functions, processes and relationships

正解: D

解説:

The most effective approach is "customised delivery of information" as per the DSCI Assessment Framework.

This ensures relevance and specificity, allowing functions, processes, and relationships to comply with the exact regulations applicable to them. General information portals or broad awareness sessions are useful but lack the precision and context that customized delivery can offer for regulatory compliance.

質問 # 95

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

正解: D

• • • • •

DCPLA無料問題: <https://www.goshiken.com/DSCI/DCPLA-mondaishu.html>

P.S. GoShikenがGoogle Driveで共有している無料かつ新しいDCPLAダンプ: <https://drive.google.com/open?>

id=1TVbdd814Bi4Kn6EFwCRbXiF6txL_8OKy