PDFVCE

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

Exam : **CIPM-Deutsch**

Title : Certified Information Privacy Manager (CIPM Deutsch Version)

Vendor : IAPP

Version : DEMO

QUESTION NO: 1
Sie möchten, dass Ihre Organisation unabhängig geprüft wird, um die Einhaltung internationaler Datenschutzstandards nachzuweisen und Lücken für die Behebung zu identifizieren.
Welche Art von Audit würde Ihnen helfen, dieses Ziel zu erreichen?
A. First-Party-Audit.
B. Second-Party-Audit.
C. Prüfung durch Dritte.
D. Viertpartei-Audit.
Answer: C
Explanation:
A third-party audit would help an organization achieve the objective of demonstrating compliance with international privacy standards and identifying gaps for remediation. A third-party audit is an audit conducted by an independent and external auditor who is not affiliated with either the audited organization or its customers. A third-party audit can provide an objective and impartial assessment of the organization's privacy practices and policies, as well as verify its compliance with relevant standards and regulations. A third-party audit can also help the organization identify areas for improvement and recommend corrective actions. A third-party audit can enhance the organization's reputation, trustworthiness, and credibility among its stakeholders and customers.
A first-party audit is an audit conducted by the organization itself or by someone within the organization who has been designated as an auditor. A first-party audit is also known as an internal audit. A first-party audit can help the organization monitor its own performance, evaluate its compliance with internal policies and procedures, and identify potential risks and opportunities for improvement. However, a first-party audit may not be sufficient to demonstrate compliance with external standards and regulations, as it may lack independence and objectivity.
A second-party audit is an audit conducted by a party that has an interest in or a relationship with the audited organization, such as a customer, a supplier, or a partner. A second-party audit is also known as an external audit. A second-party audit can help the party verify that the audited organization meets its contractual obligations, expectations, and requirements. A second-party audit can also help the party evaluate the quality and reliability of the audited organization's products or services. However, a second-party audit may not be able to provide a comprehensive and unbiased assessment of the audited organization's privacy practices and policies, as it may be influenced by the party's own interests and objectives.
References: Types of Audits: 14 Types of Audits and Level of Assurance (2022)

QUESTION NO: 2
SZENARIO
Bitte verwenden Sie Folgendes, um die nächste FRAGE zu beantworten:
Natalia, CFO der Restaurantkette Nationwide Grill, hatte ihre Kollegen noch nie so besorgt erlebt. Letzte Woche meldete eine von dem Unternehmen beauftragte Datenverarbeitungsfirma, dass ihr System möglicherweise gehackt und Kundendaten wie Namen, Adressen und Geburtstage kompromittiert wurden. Obwohl sich der Versuch als erfolglos erwiesen hat, hat die Angst mehrere Führungskräfte von Nationwide Grill dazu

veranlasst, das Datenschutzprogramm des Unternehmens auf der heutigen Sitzung in Frage zu stellen.
Alice, eine Vizepräsidentin, sagte, dass der Vorfall die Tür für Klagen hätte öffnen können, was möglicherweise die Marktposition von Nationwide Grill schädigen könnte. Der Chief Information Officer (CIO), Brendan, versuchte ihr zu versichern, dass selbst bei einem tatsächlichen Verstoß die Chancen auf eine erfolgreiche Klage gegen das Unternehmen gering seien. Aber Alice blieb nicht überzeugt.
Spencer – ein ehemaliger CEO und derzeit Senior Advisor – sagte, er habe immer vor dem Einsatz von Auftragnehmern für die Datenverarbeitung gewarnt. Er argumentierte, dass sie zumindest vertraglich dafür haftbar gemacht werden sollten, Kunden über Sicherheitsvorfälle zu informieren. Seiner Ansicht nach sollte Nationwide Grill nicht gezwungen werden, den Firmennamen für ein Problem zu beschmutzen, das es nicht verursacht hat.
Haley, eine der Führungskräfte für Geschäftsentwicklung (BD), sprach dann und flehte alle an, zur Vernunft zu kommen.
„Trotz bester Bemühungen von Organisationen kann es zu Verstößen kommen“, bemerkte sie. "Angemessene Vorbereitung ist der Schlüssel." Sie erinnerte alle an den Vorfall vor sieben Jahren, als die Finanzinformationen der großen Lebensmittelkette Tinkerton's nach einer großen Bestellung von Tiefkühlgerichten vom Nationwide Grill kompromittiert wurden. Als langjährige BD-Führungskraft mit einem soliden Verständnis der Unternehmenskultur von Tinkerton's, das durch viele Jahre der Pflege von Beziehungen aufgebaut wurde, war Haley in der Lage, die Reaktion des Unternehmens auf Vorfälle erfolgreich zu managen.
Spencer antwortete, dass vernünftiges Handeln bedeutet, dass die Sicherheit von den Sicherheitsfunktionen innerhalb des Unternehmens gehandhabt wird – nicht von BD-Mitarbeitern. In ähnlicher Weise, sagte er, müsse die Personalabteilung ihre Mitarbeiter besser schulen, um Zwischenfälle zu vermeiden. Er wies darauf hin, dass die Mitarbeiter von Nationwide Grill mit Postern, E-Mails und Memos sowohl von der Personalabteilung als auch von der Ethikabteilung im Zusammenhang mit dem Datenschutzprogramm des Unternehmens überhäuft werden. Sowohl die Menge als auch die Duplizierung von Informationen führt dazu, dass sie oft völlig ignoriert werden.
Spencer sagte: „Das Unternehmen muss sich seinem Datenschutzprogramm widmen und einmal im Monat regelmäßige persönliche Schulungen für alle Mitarbeiter veranstalten.“ Alice antwortete, dass der Vorschlag zwar gut gemeint, aber nicht praktikabel sei. Bei vielen Standorten müssen die lokalen Personalabteilungen bei ihren Schulungsplänen flexibel sein. Schweigend stimmte Natalia zu.
Der leitende Berater, Spencer, hat ein Missverständnis bezüglich?

A. Der Umfang der Verantwortung, die ein Datenverantwortlicher behält.

B. Die angemessene Rolle der Sicherheitsabteilung einer Organisation.

C. Das Ausmaß, in dem Schulungen die Anzahl der Sicherheitsvorfälle verringern können.

D. Die Rolle der Mitarbeiter der Personalabteilung im Datenschutzprogramm einer Organisation.

Answer: A
Explanation:
Spencer has a misconception regarding the amount of responsibility that a data controller retains, as he suggests that the contractors should be held contractually liable for telling customers about any security incidents, and that Nationwide Grill should not be forced to soil

the company name for a problem it did not cause. However, as a data controller, Nationwide Grill is ultimately responsible for ensuring that the personal data of its customers is processed in compliance with applicable laws and regulations, regardless of whether it uses contractors or not. Nationwide Grill cannot transfer or delegate its accountability or liability to the contractors, and it has a duty to inform the customers and the relevant authorities of any security incidents or breaches that may affect their data. Therefore, Spencer's view is unrealistic and risky, as it may expose Nationwide Grill to legal actions, fines, reputational damage and loss of trust.

QUESTION NO: 3
SZENARIO
Bitte verwenden Sie Folgendes, um die nächste FRAGE zu beantworten:
Vielleicht hätte Jack Kelly in den USA bleiben sollen. Er genießt einen hervorragenden Ruf innerhalb des Unternehmens Special Handling Shipping für seine Arbeit bei der Reformierung bestimmter "Schurken"-Büros. Letztes Jahr wurde bekannt, dass eine Geheimoperation der Polizei einen Drogenring aufgedeckt hatte, der im Büro von Providence, Rhode Island, in den Vereinigten Staaten, operierte. Videos von den Videoüberwachungskameras des Büros, die an Nachrichtenoperationen durchgesickert waren, zeigten einen Drogenaustausch zwischen Mitarbeitern von Special Handling und Undercover-Beamten.
Nach diesem Vorfall war Kelly nach Providence geschickt worden, um die „Hände weg“-Kultur zu ändern, von der das obere Management glaubte, dass sie die kriminellen Elemente ihre illegalen Transaktionen durchführen ließ. Nach ein paar Wochen unter Kellys Leitung wurde das Büro zu einem Musterbeispiel für Effizienz und Kundenservice. Kelly überwachte die Aktivitäten seiner Arbeiter mit denselben Kameras, die das illegale Verhalten ihrer ehemaligen Kollegen aufgezeichnet hatten.
Jetzt wurde Kelly damit beauftragt, das Büro in Cork, Irland, einem weiteren Krisenherd, umzudrehen. Das Unternehmen hat zahlreiche Berichte über Mitarbeiter erhalten, die das Büro unbeaufsichtigt verlassen. Als Kelly ankam, stellte er fest, dass die Mitarbeiter, selbst wenn sie anwesend waren, ihre Tage oft damit verbrachten, Kontakte zu knüpfen oder persönliche Geschäfte auf ihren Mobiltelefonen zu erledigen. Erneut beobachtete er ihr Verhalten mit Überwachungskameras. Allein aufgrund des ersten Videotages erteilte er sechs Mitarbeitern schriftliche Verweise.
Zu Kellys großer Überraschung und Verärgerung werden er und das Unternehmen nun vom irischen Datenschutzbeauftragten wegen angeblicher Verletzung der Datenschutzrechte von Mitarbeitern untersucht. Kelly wurde gesagt, dass in der Lizenz des Unternehmens für die Kameras die Gebäudesicherheit als Hauptzweck angegeben sei, aber er weiß nicht, warum das wichtig ist. Er hat seine Vorgesetzten darauf hingewiesen, dass die Schulungsprogramme des Unternehmens zum Datenschutz und zur Datenerfassung nichts über Überwachungsvideos sagen.
Sie sind ein Datenschutzberater, der vom Unternehmen beauftragt wurde, diesen Vorfall zu bewerten, über die rechtlichen und Compliance-Probleme zu berichten und die nächsten Schritte zu empfehlen.
In dem Wissen, dass die Regulierungsbehörde jetzt Ermittlungen durchführt, was wäre der beste Schritt, den man unternehmen könnte?

A. Wenden Sie sich an einen Anwalt mit Erfahrung in Datenschutzrecht und Rechtsstreitigkeiten.
B. Verwenden Sie Ihren Hintergrund und Ihr Wissen, um eine Vorgehensweise festzulegen.
C. Wenn Sie wissen, dass die Organisation schuldig ist, raten Sie ihr, die Strafe zu akzeptieren.
D. Verhandeln Sie die Bedingungen eines Vergleichs, bevor formelle rechtliche Schritte eingeleitet werden.
Answer: A
Explanation:
This answer is the best step to take knowing that the regulator is now investigating, as it can help the organization to obtain legal advice and representation on how to respond to and cooperate with the investigation, as well as how to defend or resolve any potential claims or disputes that may arise from the incident. Consulting an attorney experienced in privacy law and litigation can also help the organization to understand its rights and obligations under the applicable laws and regulations, as well as the possible outcomes and consequences of the investigation. An attorney can also assist the organization in preparing and submitting any required documents or evidence, communicating with the regulator or other parties, negotiating a settlement or agreement, or challenging or appealing any decisions or actions taken by the regulator. References: IAPP CIPM Study Guide, page 871; ISO/IEC 27002:2013, section 16.1.5

QUESTION NO: 4
Eine Organisation kann datenschutzfreundliche Technologien (PETs) zu folgenden Zwecken nutzen:
A. Aktuelle technische Kontrollen ersetzen.
B. Stärken Sie vorhandene Datenschutzkontrollen.
C. Stellen Sie die Einhaltung der lokalen Datenschutzbestimmungen sicher.
D. Erstellen Sie Daten, die vom Datenschutzexperten interpretiert werden können.
Answer: B
Explanation:
Comprehensive and Detailed Explanation:
Privacy-Enhancing Technologies (PETs) are used to strengthen existing privacy controls by improving data security, minimizing data exposure, and reducing compliance risks.
Option A (Replace current controls) is incorrect because PETs work alongside existing security measures rather than replacing them.
Option C (Ensure compliance) is incorrect because PETs help with compliance but do not guarantee it.
Option D (Produce data for interpretation) misrepresents PETs, as their primary function is protecting data rather than generating insights.
Common PETs include encryption, differential privacy, anonymization, and secure multi-party computation.
Reference:CIPM Official Textbook, Module: Privacy Technology and Security Controls - Section on Implementing Privacy-Enhancing Technologies (PETs).

QUESTION NO: 5

SZENARIO
Bitte verwenden Sie Folgendes, um die nächste FRAGE zu beantworten:
Es ist genau das, wovor du Angst hattest. Ohne Rücksprache mit Ihnen hat der IT-Direktor Ihres Unternehmens eine neue Initiative gestartet, um Mitarbeiter dazu zu ermutigen, private Geräte für die Geschäftsabwicklung zu verwenden. Die Initiative machte den Kauf eines neuen Laptops mit hoher Spezifikation zu einer attraktiven Option, da ermäßigte Laptops als Gehaltsabzug über ein Jahr Gehaltsschecks bezahlt wurden. Die Organisation zahlt auch die Umsatzsteuer. Es ist ein tolles Angebot, und nach einem Monat haben sich mehr als die Hälfte der Mitarbeiter des Unternehmens angemeldet und neue Laptops erworben. Wenn Sie durch die Einrichtung gehen, sehen Sie, wie sie fröhlich Notizen auf ihren neuen Computern anpassen und vergleichen, und am Ende des Tages nehmen die meisten ihre Laptops mit, die möglicherweise persönliche Daten zu sich nach Hause oder an andere unbekannte Orte tragen. Es'
Heute haben Sie in Ihrem Büro einen Vertreter der Marketingabteilung der Organisation, der Ihnen widerstrebend eine Geschichte mit potenziell schwerwiegenden Folgen erzählt. Am Abend zuvor ging er direkt von der Arbeit mit dem Laptop in der Hand in den Bull and Horn Pub, um mit seinen Freunden Billard zu spielen. Eine schöne Nacht voller Sport und Geselligkeit begann, während der Laptop "sicher" auf einer Bank unter seiner Jacke verstaut war. Später am Abend, als es Zeit zum Aufbruch war, holte er die Jacke, aber der Laptop war weg. Es war nicht unter der Bank oder auf einer anderen Bank in der Nähe. Der Kellner hatte es nicht gesehen. Seine Freunde spielten ihm keinen Streich. Nach einer schlaflosen Nacht bestätigte er es heute Morgen, als er in der Kneipe vorbeischaute, um mit der Reinigungsmannschaft zu sprechen. Sie hatten es nicht gefunden. Der Laptop fehlte. Gestohlen, wie es scheint. Er sieht dich an, verlegen und verärgert.
Sie fragen ihn, ob der Laptop persönliche Daten von Kunden enthält, und er nickt traurig, ja. Er glaubt, dass es Dateien von etwa 100 Kunden enthält, darunter Namen, Adressen und behördliche Identifikationsnummern. Er seufzt und stützt verzweifelt den Kopf in die Hände.
Was sollten Sie zuerst tun, um zusätzliche Informationen über den Datenverlust zu erhalten?

A. Befragen Sie die Person, die den Vorfall gemeldet hat, gemäß einem Standardprotokoll.

B. Rufen Sie die Polizei an, um Nachforschungen anzustellen, auch wenn Sie sich nicht sicher sind, ob ein Verbrechen stattgefunden hat.

C. Untersuchen Sie den Hintergrund der Person, die den Vorfall gemeldet hat.

D. Überprüfen Sie die Unternehmensaufzeichnungen der letzten Sicherungen, um festzustellen, welche Daten möglicherweise wiederhergestellt werden können.

Answer: A
Explanation:
This answer is the best way to ascertain additional information about the loss of data, as it allows you to gather relevant facts and details from the person who witnessed or experienced the incident. A standard protocol for interviewing the person reporting the incident should include questions such as:
When and where did the incident occur?
What type and amount of data was involved?
How was the data stored or protected on the laptop?
Who else had access to or knowledge of the laptop or the data?
What actions have been taken so far to recover or secure the laptop or the data?

How did you discover or report the incident?
Do you have any evidence or clues about who may have taken or accessed the laptop or the data?
Do you have any other information that may be relevant or helpful for the investigation?
Interviewing the person reporting the incident following a standard protocol can help you to establish a clear timeline and scope of the incident, identify potential sources of evidence, assess the level of risk and harm to the individuals and the organization, and determine the next steps for responding to and resolving the incident. References: IAPP CIPM Study Guide, page 87; ISO/IEC 27002:2013, section 16.1.4

QUESTION NO: 6
Der Datenschutzbeauftragte einer Organisation wurde gerade von der Sozialleistungsmanagerin darüber informiert, dass sie versehentlich den Renteneintrittsbericht aller Mitarbeiter an einen falschen Anbieter gesendet hat.
Welche der folgenden Maßnahmen sollte der Datenschutzbeauftragte zuerst ergreifen?
A. Führen Sie eine Schadensrisikoanalyse durch.
B. Melden Sie den Vorfall den Strafverfolgungsbehörden.
C. Den Empfänger kontaktieren, um die E-Mail zu löschen.
D. Firmenweite E-Mail-Benachrichtigung an Mitarbeiter senden.
Answer: A
Explanation:
The first action that the privacy officer should take after being notified by the benefits manager that she accidentally sent out the retirement enrollment report of all employees to a wrong vendor is to perform a risk of harm analysis. A risk of harm analysis is a process of assessing the potential adverse consequences for the individuals whose personal data has been compromised by a data breach or incident5 The purpose of this analysis is to determine whether the breach or incident poses a significant risk of harm to the affected individuals, such as identity theft, fraud, discrimination, physical harm, emotional distress, or reputational damage6 The risk of harm analysis should consider various factors, such as the type and amount of data involved, the sensitivity and context of the data, the likelihood and severity of harm, the characteristics of the recipients or unauthorized parties who accessed the data, and the mitigating measures taken or available to reduce the harm7 Based on this analysis, the privacy officer can then decide whether to notify the affected individuals, the relevant authorities, or other stakeholders about the breach or incident. Notification is usually required by law or best practice when there is a high risk of harm to the individuals as a result of the breach or incident8 Notification can also help to mitigate the harm by allowing the individuals to take protective actions or seek remedies. Therefore, performing a risk of harm analysis is a crucial first step for responding to a data breach or incident. References: 5: Can a risk of harm itself be a harm? | Analysis | Oxford Academic; 6: No Harm Done? Assessing Risk of Harm under the Federal Breach Notification Rule; 7: CCOHS: Hazard and Risk - Risk Assessment; 8: Breach Notification Requirements in Canada | PrivacySense.net

QUESTION NO: 7
PbD ist der Rahmen, der?
A. Bestimmt die Gestaltung des Systementwicklungslebenszyklus.

B. Legt risikobasierte Erwartungen für das Datenschutzmanagement fest.

C. Integriert Datenschutz in das Design von Technologie, Systemen und Praktiken.

D. Leitet Organisationen bei der Entwicklung, Implementierung und Verwaltung von Datenschutzprogrammen im Einklang mit Datenschutzgesetzen und bewährten Verfahren.

Answer: C

QUESTION NO: 8

Der erste Schritt, den ein Unternehmen unternehmen sollte, wenn es die Verwendung eines KI-basierten Lebenslauf-Ranking-Tools eines Drittanbieters in Erwägung zieht, ist:

A. Sichern Sie sich die Zustimmung und Genehmigung der Stakeholder, um sicherzustellen, dass das Tool die Anforderungen der Organisation erfüllt.

B. Führen Sie eine Bewertung der Auswirkungen des Tools sowohl auf den Datenschutz als auch auf die Konformität mit den geltenden KI-Vorschriften durch.

C. Verteilen Sie eine Mitteilung an die Kandidaten, deren Lebensläufe mit dem Tool bewertet werden, um sicherzustellen, dass sie die Verwendung des Tools verstehen und damit einverstanden sind.

D. Sorgen Sie für entsprechende vertragliche Zugeständnisse, um sicherzustellen, dass der Entwickler die Hauptverantwortung für etwaige Verstöße gegen geltendes Datenschutzrecht trägt.

Answer: B

Explanation:

Comprehensive and Detailed Explanation:

Before adopting an AI-based resume ranking tool, the organization must assess the tool's privacy impact and legal compliance. This ensures the company understands how the tool processes personal data and whether it introduces risks such as bias, discrimination, or non-compliance with AI and privacy regulations (e.g., GDPR, CCPA, AI Act).

Option A (Stakeholder buy-in) is important, but privacy and regulatory assessments must come first.

Option C (Notifying candidates) is a later step after ensuring compliance and assessing risks.

Option D (Contractual concessions) helps mitigate risk but does not replace due diligence in assessing compliance.

A Privacy Impact Assessment (PIA) and AI Impact Assessment should be conducted before implementation.

Reference:CIPM Official Textbook, Module: Privacy Risk and Impact Assessments - Section on Evaluating Third-Party Tools and Vendors.

QUESTION NO: 9

Zu den Anforderungen an eine Datenschutz-Folgenabschätzung (DSFA) gehört gemäß der Datenschutz-Grundverordnung (DSGVO), dass sie …

A. Der entsprechenden Aufsichtsbehörde gemeldet werden.

B. Veröffentlichen Sie den Bericht, um die Transparenz der Datenverarbeitung nachzuweisen.

C. Geben Sie eine Beschreibung des vorgeschlagenen Verarbeitungsvorgangs und seines Zwecks an.

D. Ist erforderlich, wenn die Verarbeitungstätigkeit ein Risiko für die Rechte und Freiheiten einer EU-Person mit sich bringt.

Answer: C

Explanation:

Comprehensive and Detailed Explanation:

A Data Protection Impact Assessment (DPIA) is required under Article 35 of the GDPR and must include a description of the proposed processing operation and its purpose to assess risks to data subjects.

Option A (Reported to the supervisory authority) - DPIAs are generally not reported automatically unless the risks cannot be mitigated.

Option B (Publishing the report for transparency) - While organizations should be transparent, GDPR does not require public publication of DPIAs.

Option D (Required if the activity entails risk to individuals' rights and freedoms) - This is true, but it is a condition for conducting a DPIA, not a specific requirement of the DPIA itself.

Option C (Provide a description of the proposed processing operation and its purpose) is the correct answer because Article 35 of GDPR explicitly requires this information in the DPIA.

Reference:GDPR Article 35 (DPIA Requirements) - CIPM Official Textbook, Module: Privacy Impact Assessments and Risk Management.

QUESTION NO: 10

Welche Verpflichtungen hat ein Datenverantwortlicher oder -verarbeiter gemäß der DSGVO, nachdem er einen Datenschutzbeauftragten (DSB) ernannt hat?

A. Dem DSB einen Verhaltenskodex zur Genehmigung vorlegen, der die Unternehmenspraktiken regelt und die Einhaltung der Datenschutzgrundsätze nachweisen soll.

B. Bereitstellung der notwendigen Ressourcen zur Durchführung der festgelegten Aufgaben des DSB und zur Aufrechterhaltung seines Fachwissens.

C. Um sicherzustellen, dass der DSB als einziger Ansprechpartner für Fragen von Einzelpersonen zu ihren personenbezogenen Daten fungiert.

D. Um sicherzustellen, dass der DSB ausreichende Anweisungen zur Ausübung seiner festgelegten Aufgaben erhält.

Answer: B

QUESTION NO: 11

Ein Datenschutzreifemodell bietet alles Folgende AUSSER?

A. Eine Standardreferenz zur Beurteilung des aktuellen Entwicklungsniveaus eines Datenschutzprogramms.

B. Eine Möglichkeit, hervorzuheben, welche Funktionen einem Unternehmen für ein ordnungsgemäßes Programmmanagement fehlen.

C. Eine Möglichkeit, um zu garantieren, dass ein Unternehmen die geltenden Gesetze und Vorschriften einhält.

D. Ein Beispiel für die Methoden und Praktiken, die zur Bewertung des Risikoniveaus eines Unternehmens erforderlich sind.

Answer: C

Explanation:
Comprehensive and Detailed Explanation:
A privacy maturity model helps organizations assess, benchmark, and improve their privacy programs, but it does not guarantee compliance with laws and regulations.
Option A (A standard reference to assess a privacy program's current level of development) - Maturity models provide structured frameworks for evaluation.
Option B (A way to highlight what functions a company lacks for proper program management) - Maturity models identify gaps and areas for improvement.
Option D (An example of the methods and practices necessary to evaluate a company's level of risk) - Maturity models help in risk assessment and management.
Option C (A way to guarantee compliance) is incorrect because compliance depends on actual implementation and enforcement, not just assessment.
Reference:CIPM Official Textbook, Module: Privacy Program Frameworks and Maturity Models - Section on Privacy Program Assessment and Benchmarking.

QUESTION NO: 12
Was sollte das erste große Ziel eines Unternehmens sein, das ein neues Datenschutzprogramm entwickelt?
A. Um potenzielle Finanzierungsquellen für Ressourcen des Datenschutzteams zu untersuchen.
B. Zur Planung von Gesprächen mit Führungskräften betroffener Abteilungen.
C. Um potenzielle Drittverarbeiter der Informationen der Organisation zu identifizieren.
D. Erstellung von Data Lifecycle Management-Richtlinien und -Verfahren zur Begrenzung der Datensammlung.
Answer: B
Explanation:
The first major goal of a company developing a new privacy program should be to schedule conversations with executives of affected departments. This is because a privacy program requires the support and involvement of senior management and key stakeholders from different business units, such as legal, IT, marketing, human resources, etc. By engaging with them early on, a privacy professional can understand their needs, expectations, challenges, and risks, and align the privacy program objectives and strategies with the organization's goals and culture. References: [How to Develop a Privacy Program], [Privacy Program Management]

QUESTION NO: 13
SZENARIO
Bitte verwenden Sie Folgendes, um die nächste Frage zu beantworten:
Sie sind der Datenschutzmanager im Datenschutzbüro einer National Forest Parks and Recreation Department.
Beim Mittagessen mit einem Kollegen aus der IT-Abteilung erfahren Sie, dass der IT-Direktor eine Ausschreibung für ein System zur Erfassung der personenbezogenen Daten von Parkbesuchern veröffentlicht hat.
Sie beraten sich mit einigen Kollegen aus der IT-Abteilung und erfahren, dass die Ausschreibung so formuliert ist, dass die Anbieter selbst darlegen können, welche

Informationen sie von Personen erfassen, die Parks landesweit betreten, sei es mit dem Auto oder zu Fuß. Eine unvollständige Liste der erfassten Informationen umfasst:
* persönliche Kennungen wie Name, Adresse, Alter, Geschlecht;
* Fahrzeugzulassungsinformationen:
* Gesichtsbilder von Parkbesuchern;
* Gesundheitsinformationen (z. B. körperliche Behinderungen, Verwendung von Mobilitätshilfen) Der erklärte Zweck der RFP besteht darin:
„Verbessern Sie die Fähigkeit der National Forest, Parks and Recreation Department, die Servicenutzung zu verfolgen und zu überwachen, wodurch die Zuverlässigkeit unserer Kundendaten erhöht und das Serviceangebot verbessert wird.“ Unternehmen haben bereits begonnen, Vorschläge für Softwarelösungen einzureichen, die diese Informationserfassungspraktiken berücksichtigen. Bis zum Ende der Ausschreibung ist es nur noch eine Woche.
Die IT-Abteilung hat ein RFP-Bewertungsteam zusammengestellt, aber bisher war noch niemand vom Datenschutzbeauftragten an der RFP beteiligt. Dies geschah aufgrund der Tatsache...
Was ist aus Sicht des Datenschutzmanagements am „erklärten Zweck“ der RFP problematisch?

A. Ziel ist es, die Robustheit der Kundendaten zu verbessern.

B. Ziel ist es, die Servicenutzung durch die Kunden zu verfolgen und zu überwachen.

C. Dies könnte zur unbefugten Erfassung personenbezogener Daten zur Verbesserung des Kundendienstes führen.

D. Es wird nicht angegeben, welche Informationen zur Verbesserung der Kundendaten gesammelt werden.

Answer: D

QUESTION NO: 14
Was ist das wichtigste Datenschutzziel bei der Bewertung technischer Kontrollen?

A. Zur Überprüfung und Bewertung von Lücken in gezielten internen Schulungen zum Thema Datenschutzbewusstsein.

B. Um festzustellen, ob der aktuelle Datenschutzrahmen den Anforderungen des Unternehmens entspricht.

C. Zur Bewertung und Minderung von Drittparteirisiken im Zusammenhang mit Beziehungen zu Dienstanbietern.

D. Zur Identifizierung und Minderung von Datenschutzrisiken, die mit technischen Systemen und Datenverarbeitungsaktivitäten verbunden sind.

Answer: D

QUESTION NO: 15
SZENARIO
Bitte verwenden Sie Folgendes, um die nächste FRAGE zu beantworten:
Natalia, CFO der Restaurantkette Nationwide Grill, hatte ihre Kollegen noch nie so besorgt erlebt. Letzte Woche meldete eine von dem Unternehmen beauftragte Datenverarbeitungsfirma, dass ihr System möglicherweise gehackt und Kundendaten wie Namen, Adressen und Geburtstage kompromittiert wurden. Obwohl sich der Versuch als

erfolglos erwiesen hat, hat die Angst mehrere Führungskräfte von Nationwide Grill dazu veranlasst, das Datenschutzprogramm des Unternehmens auf der heutigen Sitzung in Frage zu stellen.
Alice, eine Vizepräsidentin, sagte, dass der Vorfall die Tür für Klagen hätte öffnen können, was möglicherweise die Marktposition von Nationwide Grill schädigen könnte. Der Chief Information Officer (CIO), Brendan, versuchte ihr zu versichern, dass selbst bei einem tatsächlichen Verstoß die Chancen auf eine erfolgreiche Klage gegen das Unternehmen gering seien. Aber Alice blieb nicht überzeugt.
Spencer – ein ehemaliger CEO und derzeit Senior Advisor – sagte, er habe immer vor dem Einsatz von Auftragnehmern für die Datenverarbeitung gewarnt. Er argumentierte, dass sie zumindest vertraglich dafür haftbar gemacht werden sollten, Kunden über Sicherheitsvorfälle zu informieren. Seiner Ansicht nach sollte Nationwide Grill nicht gezwungen werden, den Firmennamen für ein Problem zu beschmutzen, das es nicht verursacht hat.
Haley, eine der Führungskräfte für Geschäftsentwicklung (BD), sprach dann und flehte alle an, zur Vernunft zu kommen. „Trotz bester Bemühungen von Organisationen kann es zu Verstößen kommen“, bemerkte sie. "Angemessene Vorbereitung ist der Schlüssel." Sie erinnerte alle an den Vorfall vor sieben Jahren, als die Finanzinformationen der großen Lebensmittelkette Tinkerton's nach einer großen Bestellung von Tiefkühlgerichten vom Nationwide Grill kompromittiert wurden. Als langjährige BD-Führungskraft mit einem soliden Verständnis der Unternehmenskultur von Tinkerton's, das durch viele Jahre der Pflege von Beziehungen aufgebaut wurde, war Haley in der Lage, die Reaktion des Unternehmens auf Vorfälle erfolgreich zu managen.
Spencer antwortete, dass vernünftiges Handeln bedeutet, dass die Sicherheit von den Sicherheitsfunktionen innerhalb des Unternehmens gehandhabt wird – nicht von BD-Mitarbeitern. In ähnlicher Weise, sagte er, müsse die Personalabteilung ihre Mitarbeiter besser schulen, um Zwischenfälle zu vermeiden. Er wies darauf hin, dass die Mitarbeiter von Nationwide Grill mit Postern, E-Mails und Memos sowohl von der Personalabteilung als auch von der Ethikabteilung im Zusammenhang mit dem Datenschutzprogramm des Unternehmens überhäuft werden. Sowohl die Menge als auch die Duplizierung von Informationen führt dazu, dass sie oft völlig ignoriert werden.
Spencer sagte: „Das Unternehmen muss sich seinem Datenschutzprogramm widmen und einmal im Monat regelmäßige persönliche Schulungen für alle Mitarbeiter veranstalten.“ Alice antwortete, dass der Vorschlag zwar gut gemeint, aber nicht praktikabel sei. Bei vielen Standorten müssen die lokalen Personalabteilungen bei ihren Schulungsplänen flexibel sein. Schweigend stimmte Natalia zu.
Was ist der realistischste Schritt, den die Organisation unternehmen kann, um die Haftung im Falle eines weiteren Vorfalls zu verringern?

A. Aufforderung an den Anbieter, regelmäßige interne Audits durchzuführen.

B. Festlegung verbindlicher Datenschutzpraktiken in Lieferantenverträgen.

C. Die Mehrheit der Verarbeitungsaktivitäten innerhalb der Organisation halten.

D. Einholen der Zustimmung des Kunden für die Verarbeitung personenbezogener Daten durch Dritte.

Answer: B
Explanation:
This answer is the most realistic step the organization can take to help diminish liability in the

event of another incident, as it can ensure that the vendor complies with the same standards and obligations as the organization regarding data protection. Vendor contracts should include clauses that specify the scope, purpose, duration and type of data processing, as well as the rights and responsibilities of both parties. The contracts should also require the vendor to implement appropriate technical and organizational measures to protect the data from unauthorized or unlawful access, use, disclosure, alteration or destruction, and to notify the organization of any security incidents or breaches. The contracts should also allow the organization to monitor, audit or inspect the vendor's performance and compliance with the contract terms and applicable laws and regulations. References: IAPP CIPM Study Guide, page 82; ISO/IEC 27002:2013, section 15.1.2

QUESTION NO: 16
Welcher Verarbeitungsvorgang würde gemäß dem Europäischen Datenschutzausschuss (EDSA) eine Datenschutz-Folgenabschätzung erfordern?
A. Eine Online-Zeitung nutzt ihre Abonnentenliste, um täglich einen Newsletter per E-Mail zu versenden.
B. Eine Gesundheitsklinik, die personenbezogene Daten ihrer Patienten in ihrem Abrechnungssystem verarbeitet.
C. Ein Krankenhaus, das die genetischen und Gesundheitsdaten von Patienten in seinem Krankenhausinformationssystem verarbeitet.
D. Ein Online-Shop, der Werbung basierend auf Artikeln anzeigt, die auf seiner eigenen Website angesehen oder gekauft wurden.
Answer: C

QUESTION NO: 17
SZENARIO
Bitte verwenden Sie Folgendes, um die nächste FRAGE zu beantworten:
Edufox hat eine jährliche Versammlung von Benutzern seiner berühmten E-Learning-Softwareplattform veranstaltet, die sich im Laufe der Zeit zu einer großartigen Veranstaltung entwickelt hat. Es füllt eines der großen Konferenzhotels in der Innenstadt und fließt in die anderen über, mit mehreren tausend Teilnehmern, die drei Tage lang Präsentationen, Podiumsdiskussionen und Networking genießen. Die Tagung ist das Kernstück des Produkt-Rollout-Zeitplans des Unternehmens und eine großartige Schulungsmöglichkeit für aktuelle Benutzer. Das Verkaufspersonal ermutigt auch potenzielle Kunden, daran teilzunehmen, um ein besseres Gefühl dafür zu bekommen, wie das System an unterschiedliche Bedürfnisse angepasst werden kann, und um zu verstehen, dass sie, wenn sie sich für dieses System entscheiden, einer Gemeinschaft beitreten, die sich wie eine Familie anfühlt.
Die diesjährige Konferenz ist nur noch drei Wochen entfernt, und Sie haben gerade von einer neuen Initiative gehört, die sie unterstützt: eine Smartphone-App für Teilnehmer. Die App wird die späte Registrierung unterstützen, die vorgestellten Präsentationen hervorheben und eine mobile Version des Konferenzprogramms bereitstellen. Es verbindet sich auch mit einem Restaurant-Reservierungssystem mit der besten Küche in den vorgestellten Bereichen. "Es wird großartig", sagt Entwicklerin Deidre Hoffman, "wenn wir es tatsächlich zum Laufen bringen!" Sie lacht nervös, erklärt aber, dass sie den Job wegen des engen Zeitrahmens, der ihr für die Entwicklung der App gegeben wurde, an eine lokale Firma

ausgelagert hat. "Es sind nur drei junge Leute", sagt sie, "aber sie leisten großartige Arbeit." Sie beschreibt einige der anderen Apps, die sie entwickelt haben. Auf die Frage, wie sie für diesen Job ausgewählt wurden, Deidre zuckt mit den Schultern. "Sie leisten gute Arbeit, also habe ich sie ausgewählt." Deidre ist eine hervorragende Mitarbeiterin mit einer starken Erfolgsbilanz. Deshalb wurde sie beauftragt, dieses überstürzte Projekt zu liefern. Sie sind sich sicher, dass ihr die besten Interessen des Unternehmens am Herzen liegen, und Sie zweifeln nicht daran, dass sie unter Druck steht, eine Frist einzuhalten, die nicht verschoben werden kann. Sie haben jedoch Bedenken hinsichtlich des Umgangs der App mit personenbezogenen Daten und ihrer Sicherheitsvorkehrungen. Beim Mittagessen im Pausenraum fängst du an, mit ihr darüber zu sprechen, aber sie versucht schnell, dich zu beruhigen: „Ich bin mir sicher, dass wir mit deiner Hilfe alle Sicherheitsprobleme beheben können, wenn es sein muss, aber ich bezweifle, dass es welche geben wird Diese Leute bauen Apps, um ihren Lebensunterhalt zu verdienen, und sie wissen, was sie tun. Sie machen sich zu viele Sorgen, aber deshalb sind Sie so gut in Ihrem Job!“

A. Aufforderung an den Anbieter, einen Fragebogen auszufüllen, der die Einhaltung der International Organization for Standardization (ISO) 27001 bewertet.

B. Durchführung einer physischen Prüfung der Einrichtungen des Anbieters.

C. Durchführung eines Penetrationstests der Datensicherheitsstruktur des Anbieters.

D. Untersuchung von Untersuchungsunterlagen zu Verstößen, die der Anbieter erlebt hat.

Answer: A

Explanation:

This answer is the best first step in understanding the data security practices of a potential vendor, as it can provide a quick and easy way to evaluate the vendor's alignment with a widely recognized and respected standard for information security management systems (ISMS). Requiring the vendor to complete a questionnaire assessing ISO 27001 compliance can help you to obtain relevant and consistent information about the vendor's data security policies, objectives, risks, controls, processes and performance. The questionnaire can also help you to compare different vendors based on their level of compliance and identify any areas that need further clarification or verification. References: IAPP CIPM Study Guide, page 82; ISO
/IEC 27002:2013, section 15.1.2

QUESTION NO: 18

Lesen Sie die folgenden Schritte:

Führen Sie häufige Datensicherungen durch.

Führen Sie Testwiederherstellungen durch, um die Integrität gesicherter Daten zu überprüfen.

Bewahren Sie gesicherte Daten offline oder auf separaten Servern auf.

Diese Schritte können einer Organisation dabei helfen, sich von was zu erholen?

A. Phishing-Angriffe

B. Autorisierungsfehler

C. Ransomware-Angriffe

D. Gestohlene Verschlüsselungsschlüssel

Answer: C

Explanation:
The steps of performing frequent data back-ups, performing test restorations to verify integrity of backed-up data, and maintaining backed-up data offline or on separate servers can help an organization recover from ransomware attacks. Ransomware is a type of malicious software that encrypts the victim's data and demands a ransom for the decryption key. Ransomware attacks can cause significant disruption, damage, and financial losses to an organization, as well as compromise the confidentiality, integrity, and availability of personal information. Having a reliable and secure backup system can help an organization restore its data and resume its operations without paying the ransom or losing valuable information.
References:
CIPM Body of Knowledge (2021), Domain IV: Privacy Program Operational Life Cycle, Section B:
Protecting Personal Information, Subsection 1: Information Security Practices CIPM Study Guide (2021), Chapter 8: Protecting Personal Information, Section 8.1: Information Security Practices CIPM Textbook (2019), Chapter 8: Protecting Personal Information, Section 8.1: Information Security Practices CIPM Practice Exam (2021), Question 129

QUESTION NO: 19
SZENARIO
Bitte verwenden Sie Folgendes, um die nächste FRAGE zu beantworten:
Henry Home Furnishings baut seit fast vierzig Jahren hochwertige Möbel. Der neue Besitzer, Anton, hat jedoch nach einem Rundgang durch die Firmenzentrale ein gewisses Maß an Desorganisation festgestellt. Sein Onkel Henry hatte sich immer auf die Produktion konzentriert – nicht auf die Datenverarbeitung – und Anton ist besorgt. In mehreren Lagerräumen hat er Papierakten, Disketten und alte Computer gefunden, die anscheinend persönliche Daten von aktuellen und ehemaligen Mitarbeitern und Kunden enthalten. Anton weiß, dass ein einziger Einbruch die Beziehung des Unternehmens zu seinen treuen Kunden unwiderruflich beschädigen könnte. Er beabsichtigt, sich das Ziel zu setzen, garantiert keinen Verlust personenbezogener Daten zu verlieren.
Zu diesem Zweck plante Anton ursprünglich, den Zugang zu den physischen Räumlichkeiten des Unternehmens zu beschränken. Allerdings will Kenneth – Vizepräsident und langjähriger Vertrauter seines Onkels – Antons Idee zurückhalten, um alle im Unternehmen aufbewahrten Papierunterlagen in elektronische Speicher umzuwandeln. Kenneth glaubt, dass dieser Prozess nur ein oder zwei Jahre dauern würde. Anton mag diese Idee; Er stellt sich ein passwortgeschütztes System vor, auf das nur er und Kenneth zugreifen können.
Anton plant außerdem, das Unternehmen von den meisten seiner Tochtergesellschaften zu trennen. Dies erleichtert nicht nur seine Arbeit, sondern vereinfacht auch die Verwaltung der gespeicherten Daten a. Die Leiter von Filialen wie der Kunstgalerie und dem Küchenartikelgeschäft um die Ecke werden für ihr eigenes Informationsmanagement verantwortlich sein. Dann können alle nicht benötigten Nebendaten, die sich noch im Besitz von Anton befinden, innerhalb der nächsten Jahre vernichtet werden.
Nachdem er von einem kürzlichen Sicherheitsvorfall erfahren hat, erkennt Anton, dass ein weiterer entscheidender Schritt die Benachrichtigung der Kunden sein wird. Kenneth beharrt darauf, dass zwei fragliche verlorene Festplatten kein Grund zur Sorge seien; Alle Daten waren verschlüsselt und nicht vertraulich. Anton will jedoch kein Risiko eingehen. Er

beabsichtigt, zur Sicherheit Mitteilungsschreiben an alle Mitarbeiter und Kunden zu senden. Anton muss auch die Einhaltung aller gesetzlichen, behördlichen und Marktanforderungen in Bezug auf den Datenschutz prüfen. Kenneth hat die Entwicklung der Online-Präsenz des Unternehmens vor etwa zehn Jahren beaufsichtigt, aber Anton ist sich nicht sicher, ob er die neuesten Online-Marketing-Gesetze versteht. Anton beauftragt einen weiteren vertrauten Mitarbeiter mit juristischem Hintergrund mit der Aufgabe der Compliance-Bewertung. Nach einer gründlichen Analyse weiß Anton, dass das Unternehmen für weitere fünf Jahre sicher sein sollte, dann kann er einen weiteren Check bestellen.
Die Dokumentation dieser Analyse zeigt die Sorgfaltspflicht der Wirtschaftsprüfer.
Anton hat einen langen Weg in Richtung einer verbesserten Führung des Unternehmens eingeschlagen, aber er weiß, dass sich der Aufwand lohnt. Anton möchte, dass das Vermächtnis seines Onkels noch viele Jahre fortbesteht.
Um das Datensicherheitssystem der Einrichtung zu verbessern, sollte Anton erwägen, den Plan für Folgendes umzusetzen?

A. Kundenkommunikation.

B. Mitarbeiterzugang zum elektronischen Speicher.

C. Mitarbeiterberatung in rechtlichen Angelegenheiten.

D. Kontrollierter Zutritt am Firmensitz.

Answer: D

Explanation:
To improve the facility's system of data security, Anton should consider following through with the plan for controlled access at the company headquarters. This plan would help to prevent unauthorized physical access to the paper files, disks, and old computers that contain personal data of employees and customers. Physical security is an important aspect of data security that involves protecting hardware and storage devices from theft, damage, or tampering1 By placing restrictions on who can enter the premises or access certain areas or rooms, Anton can reduce the risk of data breaches or incidents caused by intruders or insiders2 He can also implement locks, alarms, cameras, or guards to enhance the physical security of the facility3 References: 1: Physical Security: What Is It?; 2: [Physical Security: Why It's Important & How To Implement It]; 3: [Physical Security Best Practices: 10 Tips to Secure Your Workplace]

QUESTION NO: 20

SZENARIO
Bitte verwenden Sie Folgendes, um die nächste FRAGE zu beantworten:
Richard McAdams hat kürzlich sein Jurastudium abgeschlossen und beschlossen, in die kleine Stadt Lexington, Virginia, zurückzukehren, um die Anwaltskanzlei seines alternden Großvaters zu leiten. Der ältere McAdams wünschte sich eine begrenzte, leichtere Rolle in der Praxis, in der Hoffnung, dass sein Enkel schließlich übernehmen würde, wenn er vollständig in den Ruhestand geht. Neben der Einstellung von Richard beschäftigt Mr. McAdams zwei Rechtsanwaltsfachangestellte, einen Verwaltungsassistenten und einen Teilzeit-IT-Spezialisten, der sich um alle grundlegenden Netzwerkanforderungen kümmert. Er plant, weitere Mitarbeiter einzustellen, sobald Richard sich eingelebt hat, und bewertet die Wachstumsstrategien des Büros.
Unmittelbar nach seiner Ankunft war Richard erstaunt über die Menge an Arbeit, die getan

werden musste, um das Büro zu modernisieren, hauptsächlich im Hinblick auf den Umgang mit persönlichen Daten von Kunden. Sein erstes Ziel ist es, alle in Aktenschränken aufbewahrten Aufzeichnungen zu digitalisieren, da viele der Dokumente personenbezogene finanzielle und medizinische Daten enthalten. Außerdem ist Richard aufgefallen, dass der Verwaltungsassistent den ganzen Tag über eine enorme Menge kopiert, eine Praxis, die nicht nur täglich die Anzahl der Dateien in den Aktenschränken erhöht, sondern auch Sicherheitsprobleme verursachen kann, es sei denn, Richard hat eine formelle Richtlinie auch besorgt über die Überbeanspruchung des gemeinschaftlichen Kopierers/Druckers, der für Kunden, die das Gebäude häufig besuchen, gut sichtbar aufgestellt ist. Ein weiterer Problembereich ist die Verwendung desselben Faxgeräts durch alle Mitarbeiter.
Richard äußerte seine Besorgnis gegenüber seinem Großvater, der zustimmte, dass die Aktualisierung der Datenspeicherung, der Datensicherheit und eines Gesamtansatzes zur Erhöhung des Schutzes personenbezogener Daten in allen Facetten notwendig sei. Mr. McAdams gewährte ihm die Freiheit und Befugnis dazu. Jetzt beginnt Richard nicht nur eine Karriere als Anwalt, sondern fungiert auch als Datenschutzbeauftragter der kleinen Kanzlei.
Richard plant, sich am nächsten Tag mit dem IT-Mitarbeiter zu treffen, um einen Einblick zu erhalten, wie das Computersystem im Büro derzeit eingerichtet und verwaltet wird.
Richard muss den Lieferanten, der für die Erstellung der Datenbank der Firma verantwortlich ist, hauptsächlich aus welchem Grund genau überwachen?

A. Der Anbieter muss alle Datenschutzverletzungen den zuständigen Behörden melden.

B. Der Anbieter ist sich möglicherweise nicht der mit dem Projekt verbundenen Auswirkungen auf den Datenschutz bewusst.

C. Der Anbieter macht möglicherweise keine Angaben zu den Schwachstellen der Datenbank.

D. Der Verkäufer steht in direktem Kontakt mit allen personenbezogenen Daten der Anwaltskanzlei.

Answer: D

Explanation:
The main reason why Richard needs to closely monitor the vendor in charge of creating the firm's database is that the vendor will be in direct contact with all of the law firm's personal data. This means that the vendor will have access to sensitive and confidential information about the law firm's clients, such as their financial and medical data, which could expose them to identity theft, fraud, or other harms if mishandled or breached.
Therefore, Richard needs to ensure that the vendor follows the best practices of data protection and security, such as:
Signing a data processing agreement that specifies the scope, purpose, duration, and terms of the data processing activities, as well as the rights and obligations of both parties.
Implementing appropriate technical and organizational measures to protect the data from unauthorized or unlawful access, use, disclosure, alteration, or destruction, such as encryption, access control, backup and recovery, logging and monitoring, etc.
Complying with the relevant laws and regulations that govern the collection, use, transfer, and retention of personal data, such as the GDPR or other local privacy laws.
Reporting any data breaches or incidents to the law firm and the relevant authorities as soon as possible and taking corrective actions to mitigate the impact and prevent recurrence.
Deleting or returning the data to the law firm after the completion of the project or upon

request.

QUESTION NO: 21
Alle der folgenden Aussagen zum Einsatz technischer Sicherheitskontrollen sind richtig, AUSSER?
A. Technische Sicherheitskontrollen sind Teil einer Datenverwaltungsstrategie.
B. Technische Sicherheitskontrollen, die für eine Rechtsordnung eingesetzt werden, genügen oft auch einer anderen Rechtsordnung.
C. In den meisten Datenschutzgesetzen sind die Arten der technischen Sicherheitskontrollen aufgeführt, die implementiert werden müssen.
D. Bei der Bereitstellung technischer Sicherheitskontrollen sollte eine Person mit Sicherheitskenntnissen beteiligt sein.
Answer: C
Explanation:
Comprehensive and Detailed Explanation:
While privacy laws require appropriate technical security controls, most laws do not specify exactly which controls must be used. Instead, they mandate organizations to adopt "appropriate technical and organizational measures".
Option A (Part of data governance strategy) is correct because security controls support data protection and privacy governance.
Option B (Often satisfy multiple jurisdictions) is correct since common security measures (e.g., encryption, access controls) align with various privacy regulations.
Option D (Security expert involvement) is correct because deploying security controls requires specialized knowledge.
Reference:CIPM Official Textbook, Module: Privacy and Data Security - Section on Legal Requirements for Technical Controls.

QUESTION NO: 22
Wozu werden Datenschutz-/Sicherheitsfragebögen hauptsächlich verwendet?
A. Datenflüsse zuordnen.
B. Lieferantenrisiko bewerten.
C. Zugriffskontrollen festlegen.
D. Halten Sie die vertraglichen Anforderungen ein.
Answer: B

QUESTION NO: 23
(Alle der folgenden Punkte gehören zu den Aufgaben des Datenschutzbeauftragten, außer?)
A. Überwachung der Einhaltung von Datenschutzgesetzen und -vorschriften.
B. Durchführung von Datenschutz-Folgenabschätzungen (DSFA).
C. Definition der Datenstrategie der Organisation.
D. Sicherstellen, dass regelmäßig Datenschutzprüfungen durchgeführt werden.
Answer: C
Explanation:
CIPM defines the privacy professional's responsibilities asoversight of compliance, risk

management, PIAs, and audits. Defining the organization's data strategy is a business and executive leadership responsibility, not a privacy management function.

QUESTION NO: 24
Ein Personalleiter eines Unternehmens berichtete, dass ein Laptop mit Gehaltsdaten von Mitarbeitern im Zug verloren gegangen sei. Welche Maßnahmen sollte das Unternehmen SOFORT ergreifen?
A. Melden Sie den Diebstahl den Strafverfolgungsbehörden
B. Löschen Sie die Festplatte aus der Ferne
C. Melden Sie den Diebstahl der Geschäftsleitung
D. Führen Sie eine Multifaktor-Risikoanalyse durch
Answer: D
Explanation:
The company should perform a multi-factor risk analysis immediately after discovering the loss of the laptop containing employee payroll data. A multi-factor risk analysis is a process of assessing the potential impact and likelihood of a data breach, taking into account various factors such as the nature, scope, context, and purpose of the processing, the type and severity of the harm that may result from the breach, the number and categories of data subjects and personal data affected, the measures taken to mitigate the risk, and any relevant legal obligations or codes of conduct. A multi-factor risk analysis can help the company determine whether the breach poses a high risk to the rights and freedoms of the data subjects, and whether it needs to notify them and/or the relevant supervisory authority without undue delay, as required by Article 33 and 34 of the GDPR1. A multi-factor risk analysis can also help the company identify the root cause of the breach, evaluate the effectiveness of its existing security measures, and implement appropriate corrective actions to prevent or minimize similar incidents in the future.
References:
CIPM Body of Knowledge (2021), Domain IV: Privacy Program Operational Life Cycle, Section B:
Protecting Personal Information, Subsection 2: Data Breach Incident Planning and Management2 CIPM Study Guide (2021), Chapter 8: Protecting Personal Information, Section 8.2: Data Breach Incident Planning and Management3 CIPM Textbook (2019), Chapter 8: Protecting Personal Information, Section 8.2: Data Breach Incident Planning and Management4 CIPM Practice Exam (2021), Question 1285 GDPR Article 33 and 341

QUESTION NO: 25
Sie leiten den Bereich Datenschutz in einem mittelständischen, international tätigen B2B-Technologieunternehmen. Das Datenschutzprogramm ist bereits gut etabliert, und Sie möchten Schulungen und Sensibilisierung auf allen Unternehmensebenen verbessern und ausweiten. Sie planen eine Initiative, die den Datenschutz in bestimmten Berufsgruppen, Kategorien und Geschäftsbereichen (z. B. Entwickler, Projektmanager, Architekten) stärker in den Fokus rückt. Ihr Datenschutzteam ist jedoch klein, und Ihnen steht kein großes Budget zur Verfügung.
Sie haben ein Treffen mit der internen Kommunikationsabteilung vereinbart, um mögliche Maßnahmen zur Sensibilisierung für Datenschutz zu identifizieren und haben sich Plätze in

mehreren anstehenden Teammeetings gesichert, um dort zum Thema Datenschutz zu präsentieren. Ihr Ziel ist es, einen unternehmensweiten Sensibilisierungsplan und ein Toolkit zum Thema Datenschutz zu entwickeln, das verschiedene Stakeholder einbezieht und anschließend an die internen Fachabteilungen angepasst wird.
(Welche der folgenden Maßnahmen würde Ihnen am besten dabei helfen, die internen Stakeholder zu ermitteln, um Ihre Ziele mithilfe eines risikobasierten Ansatzes zu erreichen?)
A. Bitten Sie die Vorgesetzten, einen Mitarbeiter zur Teilnahme vorzuschlagen.
B. Führen Sie Kleingruppensitzungen durch, um die relevanten Interessengruppen zu identifizieren und zu verstehen.
C. Veröffentlichen Sie eine Nachricht auf Ihrer Website, in der Sie um Unterstützung bei Ihrem Datenschutzkonzept bitten.
D. Senden Sie eine unternehmensweite E-Mail an alle Mitarbeiter mit der Bitte um Freiwillige zur Unterstützung von Sensibilisierungskampagnen.
Answer: B
Explanation:
CIPM emphasizes using arisk-based and targeted approachwhen expanding privacy training and awareness, particularly when resources are limited. Conductingsmall group sessionsallows the privacy operations lead to identify which roles, job families, and business units process higher-risk data or engage in higher-risk activities. This method supports meaningful dialogue and helps uncover operational realities, data flows, and decision points that may not be visible through top-down nominations or broad communications.
Options A and D rely on voluntary or managerial selection, which may overlook critical but less visible stakeholders. Option C is inappropriate, as privacy awareness planning is an internal governance activity, not a public-facing initiative. Small group sessions align with CIPM guidance to embed privacy into operations by engaging stakeholders closest to the risk, ensuring training is relevant, scalable, and effective. This approach also supports the development of a reusable awareness toolkit tailored to specific operational needs, increasing long-term program maturity.

QUESTION NO: 26
SZENARIO
Bitte verwenden Sie Folgendes, um die nächste FRAGE zu beantworten:
Edufox hat eine jährliche Versammlung von Benutzern seiner berühmten E-Learning-Softwareplattform veranstaltet, die sich im Laufe der Zeit zu einer großartigen Veranstaltung entwickelt hat. Es füllt eines der großen Konferenzhotels in der Innenstadt und fließt in die anderen über, mit mehreren tausend Teilnehmern, die drei Tage lang Präsentationen, Podiumsdiskussionen und Networking genießen. Die Tagung ist das Kernstück des Produkt-Rollout-Zeitplans des Unternehmens und eine großartige Schulungsmöglichkeit für aktuelle Benutzer. Das Verkaufspersonal ermutigt auch potenzielle Kunden, daran teilzunehmen, um ein besseres Gefühl dafür zu bekommen, wie das System an unterschiedliche Bedürfnisse angepasst werden kann, und um zu verstehen, dass sie, wenn sie sich für dieses System entscheiden, einer Gemeinschaft beitreten, die sich wie eine Familie anfühlt.
Die diesjährige Konferenz ist nur noch drei Wochen entfernt, und Sie haben gerade von einer neuen Initiative gehört, die sie unterstützt: eine Smartphone-App für Teilnehmer. Die App wird die späte Registrierung unterstützen, die vorgestellten Präsentationen hervorheben und

eine mobile Version des Konferenzprogramms bereitstellen. Es verbindet sich auch mit einem Restaurant-Reservierungssystem mit der besten Küche in den vorgestellten Bereichen. "Es wird großartig", sagt Entwicklerin Deidre Hoffman, "wenn wir es tatsächlich zum Laufen bringen!" Sie lacht nervös, erklärt aber, dass sie den Job wegen des engen Zeitrahmens, der ihr für die Entwicklung der App gegeben wurde, an eine lokale Firma ausgelagert hat. "Es sind nur drei junge Leute", sagt sie, "aber sie leisten großartige Arbeit." Sie beschreibt einige der anderen Apps, die sie entwickelt haben. Auf die Frage, wie sie für diesen Job ausgewählt wurden, Deidre zuckt mit den Schultern. "Sie leisten gute Arbeit, also habe ich sie ausgewählt." Deidre ist eine hervorragende Mitarbeiterin mit einer starken Erfolgsbilanz. Deshalb wurde sie beauftragt, dieses überstürzte Projekt zu liefern. Sie sind sich sicher, dass ihr die besten Interessen des Unternehmens am Herzen liegen, und Sie zweifeln nicht daran, dass sie unter Druck steht, eine Frist einzuhalten, die nicht verschoben werden kann. Sie haben jedoch Bedenken hinsichtlich des Umgangs der App mit personenbezogenen Daten und ihrer Sicherheitsvorkehrungen. Beim Mittagessen im Pausenraum fängst du an, mit ihr darüber zu sprechen, aber sie versucht schnell, dich zu beruhigen: „Ich bin mir sicher, dass wir mit deiner Hilfe alle Sicherheitsprobleme beheben können, wenn es sein muss, aber ich bezweifle, dass es welche geben wird Diese Leute bauen Apps, um ihren Lebensunterhalt zu verdienen, und sie wissen, was sie tun. Sie machen sich zu viele Sorgen, aber deshalb sind Sie so gut in Ihrem Job!“ Sie möchten darauf hinweisen, dass die normalen Protokolle in dieser Angelegenheit NICHT befolgt wurden. Welcher Prozess wurde besonders vernachlässigt?

A. Forensische Untersuchung.

B. Datenzuordnung.

C. Verhinderung von Datenschutzverletzungen.

D. Due-Diligence-Prüfung des Anbieters.

Answer: D

Explanation:

This answer is the best way to point out that normal protocols have not been followed in this matter, as it shows that the vendor selection process was not conducted properly and that the vendor's privacy and security practices were not assessed or verified before engaging them for the app development project. Vendor due diligence vetting is a process that involves evaluating and comparing potential vendors based on their qualifications, capabilities, reputation, experience, performance and compliance with the organization's standards and expectations, as well as the applicable laws and regulations. Vendor due diligence vetting can help to ensure that the vendor can deliver the project on time, on budget and on quality, as well as protect the personal data that they process on behalf of the organization. Vendor due diligence vetting can also help to identify and mitigate any risks or issues that may arise from the vendor relationship, such as data breaches, legal actions, fines, sanctions or investigations. References: IAPP CIPM Study Guide, page 821; ISO/IEC 27002:2013, section 15.1.1

QUESTION NO: 27

Ein Antrag auf „Recht auf Löschung“ könnte abgelehnt werden, wenn die Verarbeitung personenbezogener Daten für folgende Zwecke erfolgt:

A. Ein veralteter ursprünglicher Zweck.

B. Einhaltung gesetzlicher Verpflichtungen.
C. Das Angebot von Diensten der Informationsgesellschaft.
D. Die Begründung persönlicher Rechtsansprüche.
Answer: B

QUESTION NO: 28
SZENARIO
Bitte verwenden Sie Folgendes, um die nächste FRAGE zu beantworten:
Albert arbeitet seit 15 Jahren bei Treasure Box – einem Versandhandelsunternehmen in den Vereinigten Staaten (USA), das früher dekorative Kerzen auf der ganzen Welt verkaufte, aber kürzlich beschlossen hat, seine Lieferungen an Kunden in den 48 angrenzenden Bundesstaaten zu beschränken. Trotz seiner langjährigen Erfahrung wird Albert in Führungspositionen oft übersehen. Seine Frustration darüber, nicht befördert zu werden, zusammen mit seinem jüngsten Interesse an Fragen des Datenschutzes, haben Albert motiviert, sich für positive Veränderungen einzusetzen.
Er wird sich bald für eine neu ausgeschriebene Stelle bewerben, und während des Vorstellungsgesprächs plant Albert, Führungskräfte auf Lücken im Datenschutzprogramm des Unternehmens aufmerksam zu machen. Er ist sich sicher, dass er mit einer Beförderung belohnt wird, weil er negative Folgen verhindert, die sich aus den veralteten Richtlinien und Verfahren des Unternehmens ergeben.
Albert hat zum Beispiel etwas über das Privacy Maturity Model (PMM) der AICPA (American Institute of Certified Public Accountans)/CICA (Canadian Institute of Chartered Accountants) gelernt. Albert hält das Modell für eine nützliche Methode, um die Fähigkeit von Treasure Box zum Schutz personenbezogener Daten zu messen. Albert hat festgestellt, dass Treasure Box die Anforderungen an den höchsten Reifegrad dieses Modells nicht erfüllt; Bei seinem Vorstellungsgespräch wird Albert versprechen, das Unternehmen dabei zu unterstützen, dieses Niveau zu erreichen, um den Kunden die strengsten verfügbaren Sicherheitsvorkehrungen zu bieten.
Albert möchte in seinem Vorstellungsgespräch eine positive Einstellung zeigen. Er beabsichtigt, das Engagement des Unternehmens für die Sicherheit der personenbezogenen Daten von Kunden und Mitarbeitern vor externen Bedrohungen zu loben. Allerdings macht sich Albert Sorgen um die hohe Fluktuationsrate innerhalb des Unternehmens, insbesondere im Bereich Telefondirektmarketing. Jeden Tag sieht er viele unbekannte Gesichter, die für das Marketing angeheuert werden, und er hört in der Kantine oft Beschwerden über lange Arbeitszeiten und niedrige Löhne sowie über scheinbar eklatante Missachtung der Unternehmensabläufe.
Darüber hinaus hatte Treasure Box kürzlich zwei Sicherheitsvorfälle. Das Unternehmen hat auf die Vorfälle mit internen Audits und Aktualisierungen der Sicherheitsmaßnahmen reagiert. Die Gewinne scheinen jedoch immer noch beeinträchtigt zu sein, und anekdotische Beweise deuten darauf hin, dass viele Menschen immer noch Misstrauen hegen. Albert möchte dem Unternehmen helfen, sich zu erholen. Er weiß, dass es mindestens einen Vorfall gibt, von dem die Öffentlichkeit nichts weiß, obwohl Albert die Details nicht kennt. Er glaubt, dass das Beharren des Unternehmens, den Vorfall geheim zu halten, seinem Ruf weiter schaden könnte. Ein weiterer Weg, wie Albert Treasure Box dabei helfen möchte, wieder an Bedeutung zu gewinnen, ist die Einrichtung einer gebührenfreien Nummer für Kunden sowie

ein effizienteres Verfahren zur Beantwortung von Kundenanliegen per Post.
Neben seinen Verbesserungsvorschlägen glaubt Albert, dass auch sein Wissen über die jüngsten Geschäftsmanöver des Unternehmens die Interviewer beeindrucken wird. Albert ist sich beispielsweise der Absicht des Unternehmens bewusst, in den kommenden Wochen ein Unternehmen für medizinische Versorgung zu erwerben.
Mit seinem vorausschauenden Denken hofft Albert, die Manager, die ihn interviewen werden, davon zu überzeugen, dass er der Richtige für den Job ist.
Basierend auf Alberts Beobachtungen zu den jüngsten Sicherheitsvorfällen, welche der folgenden sollte er als Priorität für Treasure Box vorschlagen?

A. Ernennung eines internen Ombudsmanns, der sich mit Beschwerden von Mitarbeitern in Bezug auf Arbeitszeit und Bezahlung befasst.

B. Einsatz eines externen Prüfers, um Datenschutzprobleme anzugehen, die bei früheren internen Prüfungen nicht erkannt wurden.

C. Zusammenarbeit mit der Personalabteilung, um die Überprüfungsverfahren für potenzielle Mitarbeiter strenger zu gestalten.

D. Bewertung der Fähigkeit des Unternehmens, mit personenbezogenen Gesundheitsdaten umzugehen, wenn der Plan zur Übernahme des Medizinbedarfsunternehmens vorangetrieben wird

Answer: B

Explanation:
This answer is the best suggestion that Albert should make based on his observations regarding recent security incidents, as it can help to ensure that Treasure Box's privacy program and practices are assessed and verified by an independent and objective party who has the necessary expertise, experience and credentials to evaluate the company's compliance with the applicable laws, regulations, standards and best practices for data protection. Using a third-party auditor can also help to identify any gaps, weaknesses or risks that may have been overlooked or missed by the prior internal audits, and to recommend or implement any improvements or corrective actions. A third-party audit can also help to enhance the company's reputation and trust among its customers, partners and stakeholders, as well as demonstrate its commitment and accountability for privacy protection.