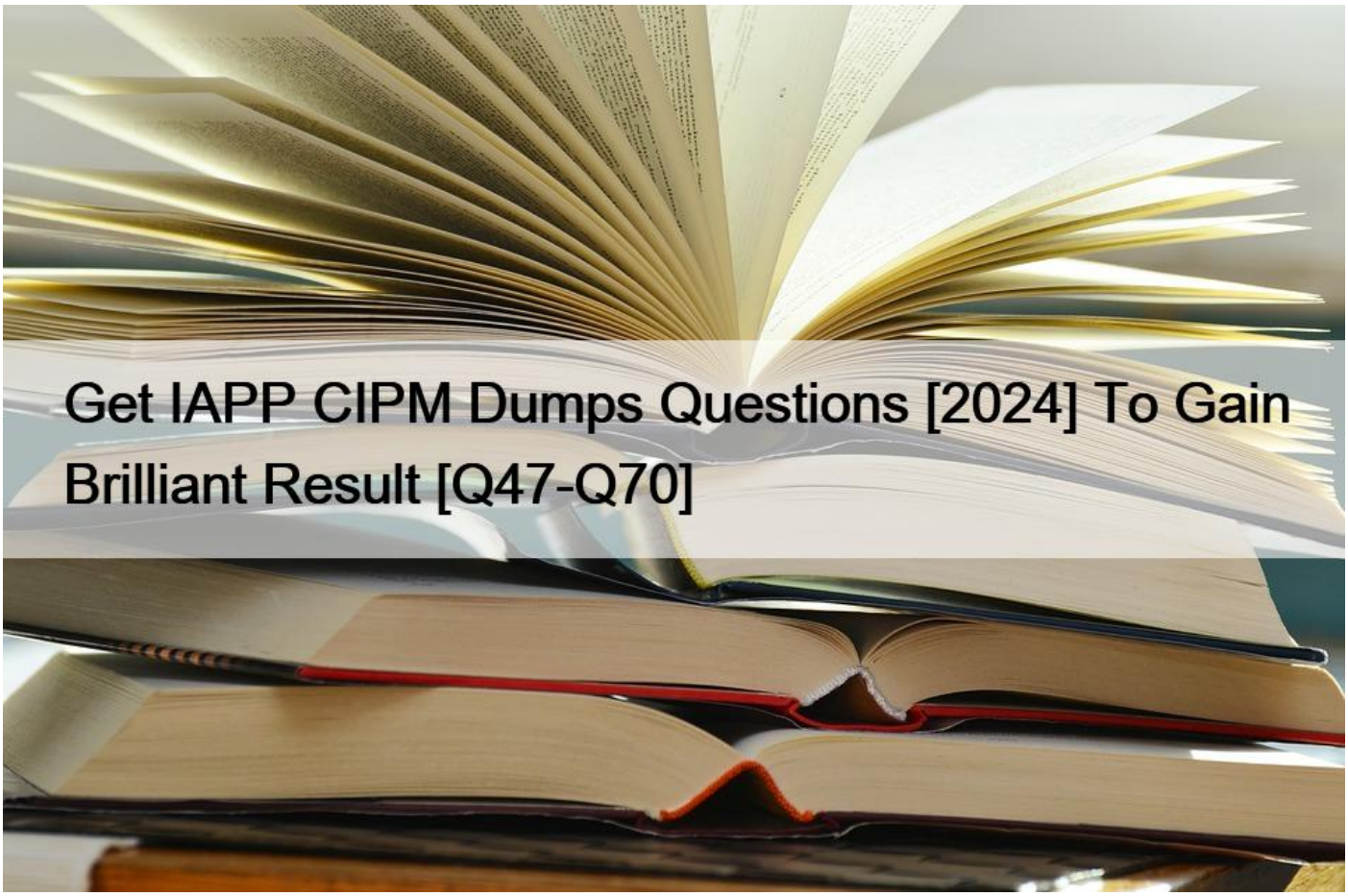
Get IAPP CIPM Dumps Questions [2024 To Gain Brilliant Result [Q47-Q70



Get IAPP CIPM Dumps Questions [2024 To Gain Brilliant Result CIPM dumps - VCEPrep - 100% Passing Guarantee

The IAPP CIPM exam is designed for professionals who have experience in managing privacy programs and want to enhance their knowledge and skills in this area. It covers a range of topics related to privacy management, including privacy laws and regulations, risk management, data governance, and compliance.

NO.47 SCENARIO

Please use the following to answer the next QUESTION:

As they company’s new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically Questionable practices, including unauthorized sales of personal data to marketers.

Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers

were thought to have been pilfered despite the company’s claims that

“appropriate” data protection safeguards were in place. The scandal affected the company’s business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard’s mentor, was forced to step down.

Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company’s board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures.

He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. “We want Medialite to have absolutely the highest standards,” he says. “In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company’s finances. So, while I want the best solutions across the board, they also need to be cost effective.” You are told to report back in a week’s time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.

The CEO likes what he’s seen of the company’s improved privacy program, but wants additional assurance that it is fully compliant with industry standards and reflects emerging best practices. What would best help accomplish this goal?
* An external audit conducted by a panel of industry experts
* An internal audit team accountable to upper management
* Creation of a self-certification framework based on company policies
* Revision of the strategic plan to provide a system of technical controls

Explanation

This approach provides an independent, unbiased review of the company’s privacy program. External experts can assess the company’s processes and controls against industry standards, benchmarks, and emerging best practices. This will not only provide the desired assurance but also potentially enhance the company’s credibility in the eyes of stakeholders, as it shows a willingness to be transparent and undergo external scrutiny.

NO.48 SCENARIO

Please use the following to answer the next QUESTION:

Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen’s line of products will only continue to grow.

With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company’s growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company’s own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.

Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that

many issues are necessary to consider before the company gets to that stage.

Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen’s CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.

Perhaps what has been most perplexing to Sadie and Amira has been the CIO’s recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.

Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.

If Amira and Sadie’s ideas about adherence to the company’s privacy policy go unchecked, the Federal Communications Commission (FCC) could potentially take action against NatGen for what?
* Deceptive practices.
* Failing to institute the hotline.
* Failure to notify of processing.
* Negligence in consistent training.

NO.49 The General Data Protection Regulation (GDPR) specifies fines that may be levied against data controllers for certain infringements. Which of the following will be subject to administrative fines of up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year?
* Failure to demonstrate that consent was given by the data subject to the processing of their personal data where it is used as the basis for processing
* Failure to implement technical and organizational measures to ensure data protection is enshrined by design and default
* Failure to process personal information in a manner compatible with its original purpose
* Failure to provide the means for a data subject to rectify inaccuracies in personal data

NO.50 SCENARIO

Please use the following to answer the next QUESTION:

Penny has recently joined Ace Space, a company that sells homeware accessories online, as its new privacy officer. The company is based in California but thanks to some great publicity from a social media influencer last year, the company has received an influx of sales from the EU and has set up a regional office in Ireland to support this expansion. To become familiar with Ace Space’s practices and assess what her privacy priorities will be, Penny has set up meetings with a number of colleagues to hear about the work that they have been doing and their compliance efforts.

Penny’s colleague in Marketing is excited by the new sales and the company’s plans, but is also concerned that Penny may curtail some of the growth opportunities he has planned. He tells her “I heard someone in the breakroom talking about some new privacy laws but I really don’t think it affects us. We’re just a small company. I mean we just sell accessories online, so what’s the real risk?” He has also told her that he works with a number of small companies that help him get projects completed in a hurry. “We’ve got to meet our deadlines otherwise we lose money. I just sign the contracts and get Jim in finance to push through the payment. Reviewing the contracts takes time that we just don’t have.” In her meeting with a member of the IT team, Penny has learned that although Ace Space has taken a number of precautions to protect its website from malicious activity, it has not taken the same level of care of its physical files or internal

infrastructure. Penny’s colleague in IT has told her that a former employee lost an encrypted USB key with financial data on it when he left. The company nearly lost access to their customer database last year after they fell victim to a phishing attack. Penny is told by her IT colleague that the IT team “didn’t know what to do or who should do what. We hadn’t been trained on it but we’re a small team though, so it worked out OK in the end.” Penny is concerned that these issues will compromise Ace Space’s privacy and data protection.

Penny is aware that the company has solid plans to grow its international sales and will be working closely with the CEO to give the organization a data “shake up”. Her mission is to cultivate a strong privacy culture within the company.

Penny has a meeting with Ace Space’s CEO today and has been asked to give her first impressions and an overview of her next steps.

To help Penny and her CEO with their objectives, what would be the most helpful approach to address her IT concerns?
* Roll out an encryption policy
* Undertake a tabletop exercise
* Ensure inventory of IT assets is maintained
* Host a town hall discussion for all IT employees

NO.51 Which term describes a piece of personal data that alone may not identify an individual?
* Unbundled data
* A singularity
* Non-aggregated infopoint
* A single attribute

Explanation

A single attribute is a term that describes a piece of personal data that alone may not identify an individual, such as a first name or a zip code. However, when combined with other attributes, it may become identifiable. References: IAPP CIPM Study Guide, page 18.

NO.52 Which of the following is an example of Privacy by Design (PbD)?
* A company hires a professional to structure a privacy program that anticipates the increasing demands of new laws.
* The human resources group develops a training program for employees to become certified in privacy policy.
* A labor union insists that the details of employers’ data protection methods be documented in a new contract.
* The information technology group uses privacy considerations to inform the development of new networking software.

Explanation

This is an example of Privacy by Design (PbD), which is an approach to systems engineering that integrates privacy into the design and development of products, services, and processes from the outset7 PbD aims to ensure that privacy is embedded into the core functionality of any system or service, rather than being added as an afterthought or a trade-off. PbD is based on seven foundational principles: proactive not reactive; preventive not remedial; privacy as the default setting; privacy embedded into design; full functionality – positive-sum, not zero-sum; end-to-end security – full lifecycle protection; visibility and transparency – keep it open; and respect for user privacy – keep it user-centric8

NO.53 For an organization that has just experienced a data breach, what might be the least relevant metric for a company’s privacy and governance team?
* The number of security patches applied to company devices.
* The number of privacy rights requests that have been exercised.
* The number of Privacy Impact Assessments that have been completed.
* The number of employees who have completed data awareness training.

NO.54 SCENARIO

Please use the following to answer the next QUESTION:

Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain “rogue” offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office’s video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.

In the wake of this incident, Kelly had been sent to Providence to change the “hands off” culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly’s direction, the office became a model of efficiency and customer service. Kelly monitored his workers’ activities using the same cameras that had recorded the illegal conduct of their former co-workers.

Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.

Much to Kelly’s surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company’s license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company’s training programs on privacy protection and data collection mention nothing about surveillance video.

You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.

What does this example best illustrate about training requirements for privacy protection?
* Training needs must be weighed against financial costs.
* Training on local laws must be implemented for all personnel.
* Training must be repeated frequently to respond to new legislation.
* Training must include assessments to verify that the material is mastered.

NO.55 SCENARIO

Please use the following to answer the next question:

Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company’s product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.

This year’s conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. “It’s going to be great,” the developer, Deidre Hoffman, tells you, “if, that is, we actually get it working!” She laughs nervously but explains that because of the tight time frame she’d been given to build the app, she outsourced the job to a local firm. “It’s just three young people,” she says, “but they do great

work.” She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. “They do good work, so I chose them.” Deidre is a terrific employee with a strong track record. That’s why she’s been charged to deliver this rushed project. You’re sure she has the best interests of the company at heart, and you don’t doubt that she’s under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app’s handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, “I’m sure with your help we can fix any security issues if we have to, but I doubt there’ll be any. These people build apps for a living, and they know what they’re doing. You worry too much, but that’s why you’re so good at your job!” You want to point out that normal protocols have not been followed in this matter. Which process in particular has been neglected?

* Forensic inquiry
* Data mapping
* Privacy breach prevention
* Vendor due diligence or vetting

NO.56 SCENARIO

Please use the following to answer the next QUESTION:

It’s just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It’s a great deal, and after a month, more than half the organization’s employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them, potentially carrying personal data to their homes or other unknown locations. It’s enough to give you data- protection nightmares, and you’ve pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.

Today you have in your office a representative of the organization’s marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop “safely” tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.

You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.

Which is the best way to ensure that data on personal equipment is protected?

* User risk training.
* Biometric security.
* Encryption of the data.
* Frequent data backups.

NO.57 What does it mean to “rationalize” data protection requirements?

* Evaluate the costs and risks of applicable laws and regulations and address those that have the greatest penalties
* Look for overlaps in laws and regulations from which a common solution can be developed
* Determine where laws and regulations are redundant in order to eliminate some from requiring compliance

* Address the less stringent laws and regulations, and inform stakeholders why they are applicable

Explanation

To rationalize data protection requirements means to look for overlaps in laws and regulations from which a common solution can be developed. This can help simplify compliance efforts and reduce costs and complexity. References: IAPP CIPM Study Guide, page 16.

NO.58 Formosa International operates in 20 different countries including the United States and France. What organizational approach would make complying with a number of different regulations easier?

* Data mapping.
* Fair Information Practices.
* Rationalizing requirements.
* Decentralized privacy management.

NO.59 SCENARIO

Please use the following to answer the next QUESTION:

Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company’s flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments.

After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.

The packaging and user guide for the Handy Helper indicate that it is a “privacy friendly” product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.

Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the Questions as he was not involved in the product development process.

In speaking with the product team, he learned that the Handy Helper collected and stored all of a user’s sensitive medical information for the medical appointment scheduler. In fact, all of the user’s information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.

Consistent with the CEO’s philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.

What administrative safeguards should be implemented to protect the collected data while in use by Manasa and her product management team?

* Document the data flows for the collected data.
* Conduct a Privacy Impact Assessment (PIA) to evaluate the risks involved.
* Implement a policy restricting data access on a “need to know” basis.
* Limit data transfers to the US by keeping data collected in Europe within a local data center.

Explanation

An administrative safeguard that should be implemented to protect the collected data while in use by Manasa and her product management team is a policy restricting data access on a “need to know” basis. This means that only authorized personnel who have a legitimate business purpose for accessing the data should be able to do so3 This would help to prevent unauthorized or unnecessary access, use, or disclosure of sensitive or personal data by internal or external parties. It would also reduce the risk of data breaches, theft, or loss that could compromise the confidentiality, integrity, and availability of the data4 References: 3: HIPAA Security Series #2 – Administrative Safeguards – HHS.gov; 4: Administrative Safeguards of the Security Rule: What Are They?

NO.60 SCENARIO

Please use the following to answer the next question:

Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company’s flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments.

After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.

The packaging and user guide for the Handy Helper indicate that it is a “privacy friendly” product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.

Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Question about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the Question as he was not involved in the product development process.

In speaking with the product team, he learned that the Handy Helper collected and stored all of a user’s sensitive medical information for the medical appointment scheduler. In fact, all of the user’s information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.

Consistent with the CEO’s philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called “Eureka.” Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.

What security controls are missing from the Eureka program?
* Storage of medical data in the cloud is not permissible under the General Data Protection Regulation (GDPR)
* Data access is not limited to those who “need to know” for their role
* Collection of data without a defined purpose might violate the fairness principle
* Encryption of the data at rest prevents European users from having the right of access and the right of portability of their data

NO.61 SCENARIO

Please use the following to answer the next QUESTION:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production – not data processing – and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company’s relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.

To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth – his uncle’s vice president and longtime confidante – wants to hold off on Anton’s idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password- protected system that only he and Kenneth can access.

Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton’s possession can be destroyed within the next few years.

After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.

Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company’s online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.

Documentation of this analysis will show auditors due diligence.

Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle’s legacy to continue for many years to come.

In terms of compliance with regulatory and legislative changes, Anton has a misconception regarding?
* The timeline for monitoring.
* The method of recordkeeping.
* The use of internal employees.
* The type of required qualifications.

Explanation

In terms of compliance with regulatory and legislative changes, Anton has a misconception regarding the timeline for monitoring. He believes that the company should be safe for another five years after conducting a compliance assessment and documenting the analysis. However, this is a risky and unrealistic assumption that could expose the company to legal liabilities and penalties. Regulatory and legislative changes are dynamic and frequent in today’s business environment. They can affect various aspects of the company’s operations, such as data protection, online marketing, consumer rights, labor laws, tax laws, environmental laws, etc5 Therefore, the company needs to monitor these changes continuously and proactively to ensure compliance at all times. Waiting for five years to check for compliance again could result in missing important updates or requirements that could impact the company’s business practices or obligations. Moreover, compliance monitoring is not only a one-time activity but an ongoing process that involves evaluating the effectiveness of the company’s policies and procedures in meeting the regulatory standards and expectations6 Compliance monitoring also helps to identify any gaps or weaknesses in the company’s compliance program and take corrective actions to improve it. Therefore, Anton should revise his timeline for

monitoring regulatory and legislative changes and adopt a more regular and systematic approach that aligns with the company’s risk profile and regulatory environment. References: 5: Regulatory Change Management:

How To Keep Up With Regulatory Changes; 6: Compliance Monitoring – What Is It?

NO.62 Under the General Data Protection Regulation (GDPR), when would a data subject have the right to require the erasure of his or her data without undue delay?
* When the data subject is a public authority
* When the erasure is in the public interest
* When the processing is carried out by automated means
* When the data is no longer necessary for its original purpose

NO.63 When supporting the business and data privacy program expanding into a new jurisdiction, it is important to do all of the following EXCEPT?
* Identify the stakeholders.
* Appoint a new Privacy Officer (PO) for that jurisdiction.
* Perform an assessment of the laws applicable in that new jurisdiction.
* Consider culture and whether the privacy framework will need to account for changes in culture.

Explanation

When expanding into a new jurisdiction, it is not necessary to appoint a new Privacy Officer (PO) for that jurisdiction, unless the local law requires it. The other options are important steps to ensure compliance with the new jurisdiction’s privacy laws and regulations, as well as to align the privacy program with the business objectives and culture of the new market. References: CIPM Body of Knowledge, Domain I: Privacy Program Governance, Task 1: Establish the privacy program vision and strategy.

NO.64 What should a privacy professional keep in mind when selecting which metrics to collect?
* Metrics should be reported to the public.
* The number of metrics should be limited at first.
* Metrics should reveal strategies for increasing company earnings.
* A variety of metrics should be collected before determining their specific functions.

Explanation/Reference:

NO.65 SCENARIO

Please use the following to answer the next QUESTION:

Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company’s flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments.

After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.

The packaging and user guide for the Handy Helper indicate that it is a “privacy friendly” product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.

Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Questions about the product from the distributor. Sanjay needed to look more closely at the product in order

to be able to answer the Questions as he was not involved in the product development process.

In speaking with the product team, he learned that the Handy Helper collected and stored all of a user’s sensitive medical information for the medical appointment scheduler. In fact, all of the user’s information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.

Consistent with the CEO’s philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.

What administrative safeguards should be implemented to protect the collected data while in use by Manasa and her product management team?
* Document the data flows for the collected data.
* Conduct a Privacy Impact Assessment (PIA) to evaluate the risks involved.
* Implement a policy restricting data access on a “need to know” basis.
* Limit data transfers to the US by keeping data collected in Europe within a local data center.

NO.66 SCENARIO

Please use the following to answer the next QUESTION:

Ben works in the IT department of IgNight, Inc., a company that designs lighting solutions for its clients. Although IgNight’s customer base consists primarily of offices in the US, some individuals have been so impressed by the unique aesthetic and energy-saving design of the light fixtures that they have requested IgNight’s installations in their homes across the globe.

One Sunday morning, while using his work laptop to purchase tickets for an upcoming music festival, Ben happens to notice some unusual user activity on company files. From a cursory review, all the data still appears to be where it is meant to be but he can’t shake off the feeling that something is not right. He knows that it is a possibility that this could be a colleague performing unscheduled maintenance, but he recalls an email from his company’s security team reminding employees to be on alert for attacks from a known group of malicious actors specifically targeting the industry.

Ben is a diligent employee and wants to make sure that he protects the company but he does not want to bother his hard-working colleagues on the weekend. He is going to discuss the matter with this manager first thing in the morning but wants to be prepared so he can demonstrate his knowledge in this area and plead his case for a promotion.

Going forward, what is the best way for IgNight to prepare its IT team to manage these kind of security events?
* Tabletop exercises.
* Update its data inventory.
* IT security awareness training.
* Share communications relating to scheduled maintenance.

NO.67 What is the main purpose in notifying data subjects of a data breach?
* To avoid financial penalties and legal liability
* To enable regulators to understand trends and developments that may shape the law
* To ensure organizations have accountability for the sufficiency of their security measures
* To allow individuals to take any actions required to protect themselves from possible consequences

Explanation

The main purpose in notifying data subjects of a data breach is to allow individuals to take any actions required to protect themselves from possible consequences, such as identity theft, fraud, or discrimination.

This is consistent with the principle of transparency and the right to information under the GDPR. The other options are not the main purpose of notification, although they may be secondary effects or benefits of the process. References:

* Data protection impact assessments | ICO

* [Art. 34 GDPR – Communication of a personal data breach to the data subject – GDPR.eu]

NO.68 You would like your organization to be independently audited to demonstrate compliance with international privacy standards and to identify gaps for remediation.

Which type of audit would help you achieve this objective?
* First-party audit.
* Second-party audit.
* Third-party audit.
* Fourth-party audit.

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)

NO.69 What is one reason the European Union has enacted more comprehensive privacy laws than the United States?
* To ensure adequate enforcement of existing laws
* To ensure there is adequate funding for enforcement
* To allow separate industries to set privacy standards
* To allow the free movement of data between member countries

Explanation/Reference:

NO.70 SCENARIO

Please use the following to answer the next QUESTION:

Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather’s law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office’s strategies for growth.

Immediately upon arrival, Richard was amazed at the amount of work that needed to done in order to modernize the office, mostly in regard to the handling of clients’ personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place Richard is also concerned with the overuse of the communal copier/ printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year’s end.

Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary Mr. McAdams granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.

Which of the following policy statements needs additional instructions in order to further protect the personal data of their clients?
* All faxes sent from the office must be documented and the phone number used must be double checked to ensure a safe arrival.
* All unused copies, prints, and faxes must be discarded in a designated recycling bin located near the work station and emptied daily.
* Before any copiers, printers, or fax machines are replaced or resold, the hard drives of these devices must be deleted before leaving the office.
* When sending a print job containing personal data, the user must not leave the information visible on the computer screen following the print command and must retrieve the printed document immediately.
Explanation

The policy statement that needs additional instructions in order to further protect the personal data of their clients is: All unused copies, prints, and faxes must be discarded in a designated recycling bin located near the work station and emptied daily. This policy statement is insufficient because it does not specify how the unused copies, prints, and faxes should be discarded. Simply throwing them into a recycling bin may expose them to unauthorized access or theft by anyone who has access to the bin or its contents. Furthermore, emptying the bin daily may not be frequent enough to prevent accumulation or overflow of sensitive documents.

To further protect the personal data of their clients, this policy statement should include additional instructions such as:

* All unused copies, prints, and faxes must be shredded before being discarded in a designated recycling bin located near the work station.

* The recycling bin must be locked or secured at all times when not in use.

* The recycling bin must be emptied at least twice a day or whenever it is full.

These additional instructions would ensure that the unused copies, prints, and faxes are destroyed in a secure manner and that the recycling bin is not accessible to unauthorized persons or prone to overflow.

The other policy statements do not need additional instructions, as they already provide adequate measures to protect the personal data of their clients. Documenting and double-checking the phone number for faxes ensures that the faxes are sent to the correct and intended recipient. Deleting the hard drives of copiers, printers, or fax machines before replacing or reselling them prevents data leakage or recovery by third parties.

Not leaving the information visible on the computer screen and retrieving the printed document immediately prevents data exposure or theft by anyone who can see the screen or access the printer.

The Certified Information Privacy Manager (CIPM) certification is offered by the International Association of Privacy Professionals (IAPP), which is the largest and most comprehensive global information privacy community. The IAPP CIPM Certification Exam covers topics such as privacy program governance, privacy risk assessment, privacy policies and notices, training and awareness, and privacy audits. It is a rigorous exam that requires candidates to demonstrate their understanding of privacy laws and regulations, as well as their ability to implement effective privacy management strategies in organizations of all sizes and types. Certified Information Privacy Manager (CIPM) certification is highly valued by employers and can help professionals advance their careers in the field of privacy management.