CIPM Q&As

Certified Information Privacy Manager

Pass IAPP CIPM Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cipm.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

SCENARIO Please use the following to answer the next QUESTION: Natalia, CFO of the Nationwide Grill restaurant chain, had never seen her fellow executives so anxious. Last week, a data processing firm used by the company reported that its system may have been hacked, and customer data such as

names, addresses, and birthdays may have been compromised. Although the attempt was proven unsuccessful, the scare has prompted several Nationwide Grill executives to Question the company\\'s privacy program at today\\'s meeting.

Alice, a vice president, said that the incident could have opened the door to lawsuits, potentially damaging Nationwide Grill\\'s market position. The Chief Information Officer (CIO), Brendan, tried to assure her that even if there had been an actual breach, the chances of a successful suit against the company were slim. But Alice remained unconvinced. Spencer ?a former CEO and currently a senior advisor ?said that he had always warned against the use of contractors for data processing. At the very least, he argued, they should be held contractually liable for telling customers about any

security incidents. In his view, Nationwide Grill should not be forced to soil the company name for a problem it did not cause.

One of the business development (BD) executives, Haley, then spoke, imploring everyone to see reason. "Breaches can happen, despite organizations\\' best efforts," she remarked. "Reasonable preparedness is key." She reminded everyone

of the incident seven years ago when the large grocery chain Tinkerton\\'s had its financial information compromised after a large order of Nationwide Grill frozen dinners. As a long-time BD executive with a solid understanding of Tinkerton\\'s\\'s corporate culture, built up through many years of cultivating relationships, Haley was able to successfully manage the company\\'s incident response. Spencer replied that acting with reason means allowing security to be handled by the security functions within the company ?not BD staff. In a similar way, he said, Human Resources (HR) needs to do a better job training employees to

prevent incidents. He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company\\'s privacy program. Both the volume and the duplication of information means that it is often ignored altogether.

Spencer said, "The company needs to dedicate itself to its privacy program and set regular in-person trainings for all staff once a month."

Alice responded that the suggestion, while well-meaning, is not practical. With many locations, local HR departments need to have flexibility with their training schedules.

Silently, Natalia agreed.

Based on the scenario, Nationwide Grill needs to create better employee awareness of the company\\'s privacy program by doing what?

A. Varying the modes of communication.

B. Communicating to the staff more often.

C. Improving inter-departmental cooperation.

D. Requiring acknowledgment of company memos.

Correct Answer: D

QUESTION 2

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. You are charged with making sure that privacy safeguards are in place for new products and initiatives. What is the best way to do this?

A. Hold a meeting with stakeholders to create an interdepartmental protocol for new initiatives

B. Institute Privacy by Design principles and practices across the organization

C. Develop a plan for introducing privacy protections into the product development stage

D. Conduct a gap analysis after deployment of new products, then mend any gaps that are revealed

Correct Answer: C

QUESTION 3

SCENARIO

Please use the following to answer the next QUESTION:

John is the new privacy officer at the prestigious international law firm ?and;M LLP. and;M LLP is very proud of its reputation in the practice areas of Trusts and Estates and Merger and Acquisition in both U.S. and Europe.

During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm\\'s email continuity service to their existing email security vendor ?MessageSafe. Being

successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from

Cloud Inc. to host email continuity service for AandM LLP.

John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe\\'s previous breach and learned that the breach was

caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.

At the meeting, Derrick emphasized that email is the primary method for the firm\\'s lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the

anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up

the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn\\'t have the time or resource to look for

another solution. Furthermore, the off- premises email continuity service will only be turned on when the email service at AandM LLP\\'s primary and secondary data centers are both down, and the email messages stored at MessageSafe site for

continuity service will be automatically deleted after 30 days.

Which of the following is a TRUE statement about the relationship among the organizations?

A. Cloud Inc. must notify AandM LLP of a data breach immediately.

B. MessageSafe is liable if Cloud Inc. fails to protect data from AandM LLP.

C. Cloud Inc. should enter into a data processor agreement with AandM LLP.

D. AandM LLP\\'s service contract must be amended to list Cloud Inc. as a sub-processor.

Correct Answer: A

QUESTION 4

What is a key feature of the privacy metric template adapted from the National Institute of Standards and Technology (NIST)?

A. It provides suggestions about how to collect and measure data.

B. It can be tailored to an organization\\'s particular needs.

C. It is updated annually to reflect changes in government policy.

D. It is focused on organizations that do business internationally.

Correct Answer: A

QUESTION 5

Your company wants to convert paper records that contain customer personal information into electronic form, upload the records into a new third-party marketing tool and then merge the customer personal information in the marketing tool with information from other applications.

As the Privacy Officer, which of the following should you complete to effectively make these changes?

A. A Record of Authority.

B. A Personal Data Inventory.

C. A Privacy Threshold Analysis (PTA).

D. A Privacy Impact Assessment (PIA).

Correct Answer: B

QUESTION 6

SCENARIO

Please use the following to answer the next question:

Felicity is the Chief Executive Officer (CEO) of an international clothing company that does business in several countries, including the United States (U.S.), the United Kingdom (UK), and Canada. For the first five years under Felicity\\'s

leadership, the company was highly successful due its higher profile on the Internet via target advertising and the use of social media. However, business has dropped in recent months, and Felicity is looking to cut costs across all

departments.

She has prepared to meet with the Chief Information Officer (CIO), Jin, who is also head of the company\\'s privacy program.

After reviewing many of Jin\\'s decisions, Felicity firmly believes that, although well-intentioned, Jin overspends company resources. Felicity has taken several notes on ways she believes the company can spend less money trying to uphold its

privacy mission. First, Felicity intends to discuss the size of the company\\'s information security budget with Jin. Felicity proposes to streamline information security by putting it solely within the purview of the company\\'s Information Technology

(IT) experts, since personal data within the company is stored electronically.

She is also perplexed by the Privacy Impact Assessments (PIAs) Jin facilitated at some of the company\\'s locations. Jin carefully documented the approximate amount of man-hours the PIAs took to complete, and Felicity is astounded at the

amount. She cannot understand why so much time has been spent on sporadic PIAs.

Felicity has also recently received complaints from employees, including mid-level managers, about the great burden of paperwork necessary for documenting employee compliance with the company\\'s privacy policy. She hopes Jin can

propose cheaper, more efficient ways of monitoring compliance. In Felicity\\'s view, further evidence of Jin\\'s

overzealousness is his insistence on monitoring third-party processors for their observance of the company\\'s privacy policy. New staff

members seem especially overwhelmed. Despite the consistent monitoring, two years ago the company had to pay remediation costs after a security breach of a processor\\'s data system. Felicity wonders whether processors can be held

contractually liable for the costs of any future breaches.

Last in Felicity\\'s notes is a reminder to discuss Jin\\'s previous praise for the company\\'s independent ethics function within the Human Resources (HR) department. Felicity believes that much company time could be saved if the Ethics Officer

position were done away with, and that any ethical concerns were simply brought directly to the executive leadership of the company.

Although Felicity questions many of Jin\\'s decisions, she hopes that their meeting will be productive and that Jin, who is widely respected throughout the company, will help the company save money. Felicity believes that austerity is the only

way forward.

Based on Felicity\\'s intended changes, which of the following is most likely to be of concern to Jin regarding the safety of personal data?

A. The impacts of online marketing.

B. The effective use of several types of controls.

C. The wording of the company\\'s privacy notice.

D. The rigor of the company\\'s various hiring practices.

Correct Answer: B

QUESTION 7

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?

A. Implement audit logging and monitoring tools.

B. Ensure an inventory of IT assets is maintained.

C. Host a town hall discussion for all IT employees to delivery necessary training.

D. Perform a gap analysis of the technical countermeasures required to meet privacy compliance.

Correct Answer: A

QUESTION 8

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!"

Since it is too late to restructure the contract with the vendor or prevent the app from being deployed, what is the best step for you to take next?

A. Implement a more comprehensive suite of information security controls than the one used by the vendor.

B. Ask the vendor for verifiable information about their privacy protections so weaknesses can be identified.

C. Develop security protocols for the vendor and mandate that they be deployed.

D. Insist on an audit of the vendor\\'s privacy procedures and safeguards.

Correct Answer: B

QUESTION 9

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?

A. The timeline for monitoring.

B. The method of recordkeeping.

C. The use of internal employees.

D. The type of required qualifications.

Correct Answer: B

QUESTION 10

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.

What is the best way for Penny to understand the location, classification and processing purpose of the personal data Ace Space has?

A. Analyze the data inventory to map data flows

B. Audit all vendors\\' privacy practices and safeguards

C. Conduct a Privacy Impact Assessment for the company

D. Review all cloud contracts to identify the location of data servers used

Correct Answer: B

QUESTION 11

Which of the following is the optimum first step to take when creating a Privacy Officer governance model?

A. Involve senior leadership.

B. Provide flexibility to the General Counsel Office.

C. Develop internal partnerships with IT and information security.

D. Leverage communications and collaboration with public affairs teams.

Correct Answer: C

QUESTION 12

SCENARIO

Please use the following to answer the next question:

Hi Zoe,

Thank you so much for your email. I am so glad you have jumped right into your new position as our in-house privacy professional. BastTech greatly needs your expertise. I hope you are comfortably settling into your new home in the United

States after your move from the United Kingdom! Georgia is a wonderful state.

I particularly appreciate your enthusiasm in using your recent informal assessment to begin rectifying gaps in our privacy program and making sure we are in compliance with all laws. However, I also want to make sure that we are prioritizing

our initiatives by spending time on the measures that are most important to our customers, our company, and the tech industry as a whole.

Specifically, I know that you are advocating for an update of our Business Continuity Disaster Response (BCDR) plan with an eye toward privacy concerns. I think this effort is something that we may be able to postpone. I\\'m sure that after ten

years the document can be updated in spots; however, we have first-rate, experienced executive leaders that would have things well in hand in the unlikely event of a disaster.

Further, you mentioned that you would like to assess our longtime subcontractor\\'s disaster plan through a second-party audit. Papyrus, our longtime subcontractor, does keep a great deal of personal data about our customers. However, I am

not sure I understand your request and would like to discuss this further during our meeting Wednesday.

You also say that your audit uncovered some inadequacies in staff compliance with our security procedures and local laws. I just wanted to emphasize that the audit findings only need to be communicated to the executive leadership. I would

rather not cause unnecessary alarm across departments.

I know you are also looking closely at the recent loss of a file belonging to a staff member in Human Resources (HR). It was an unfortunate incident, but rest assured, we handled the situation according to Georgia state law. The only difficult part was easing the concerns of our many remote employees all across the country whose data was on the computer. But I believe everything is settled. At least this stands as proof that in the event of another breach of any type, Information Security (IS) will take the lead while other departments move on with business as usual without having to get involved. Thankfully, we have taken the measure of supplementing our General Commercial Liability Insurance with cyber insurance.

Anyway, we will talk more on Wednesday. I just wanted to communicate some of my current thinking.

Thanks,

Whitney

Interim Assistant Business Manager, BastTech.

Based on the email, what should Zoe suggest to Whitney regarding the informal audit?

A. That several audits be conducted in quick succession.

B. That the results of the audit eventually be made public.

C. That more people assist with conducting audits in the future.

D. That the information from the audit be disseminated to key personnel.

Correct Answer: D

QUESTION 13

SCENARIO

Please use the following to answer the next QUESTION:

As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your

accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.

You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program\\'s sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.

Initially, your work was greeted with little confidence or enthusiasm by the company\\'s "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other

employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.

Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is

fairly effective.

You are left contemplating:

What must be done to maintain the program and develop it beyond just a data breach prevention program? How can you build on your success?

What are the next action steps?

What stage of the privacy operational life cycle best describes Consolidated\\'s current privacy program?

A. Assess.

B. Protect.

C. Respond.

D. Sustain.

Correct Answer: D

QUESTION 14

What is the main reason to begin with 3-5 key metrics during the program development process?

A. To avoid undue financial costs.

B. To keep the focus on the main organizational objectives.

C. To minimize selective data use.

D. To keep the process limited to as few people as possible.

Correct Answer: C

QUESTION 15

A company has started developing a privacy program. The Data Protection Officer (DPO) has been working long hours to develop cohesive procedures and processes; however, he failed to fully document each aspect of the data retention process. Which level from the Privacy Maturity Model most closely describes the company?

A. Ad Hoc.

B. Defined.

C. Managed.

D. Repeatable.

Correct Answer: A